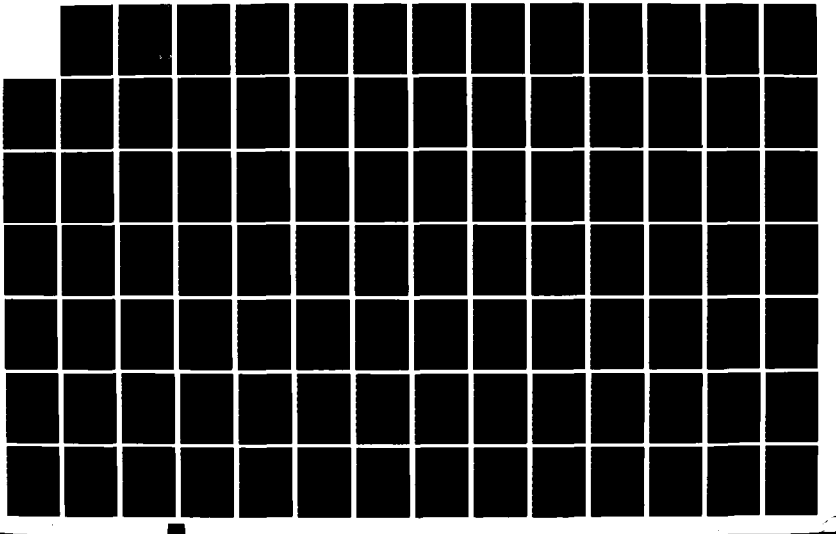
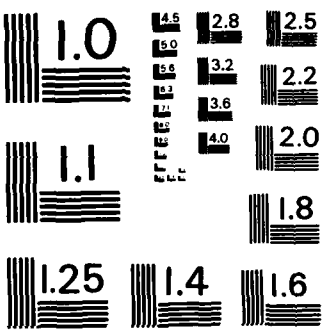
AD-A161 332 INTERFACING THE DEFENSE STANDARD AMMUNITION COMPUTER SYSTEM AND THE AIR F.. (U) AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH SCHOOL OF SYST.. A C JONES

1/2

UNCLASSIFIED SEP 85 AFIT/GLM/LSM/85S-39 F/G 15/5 NL

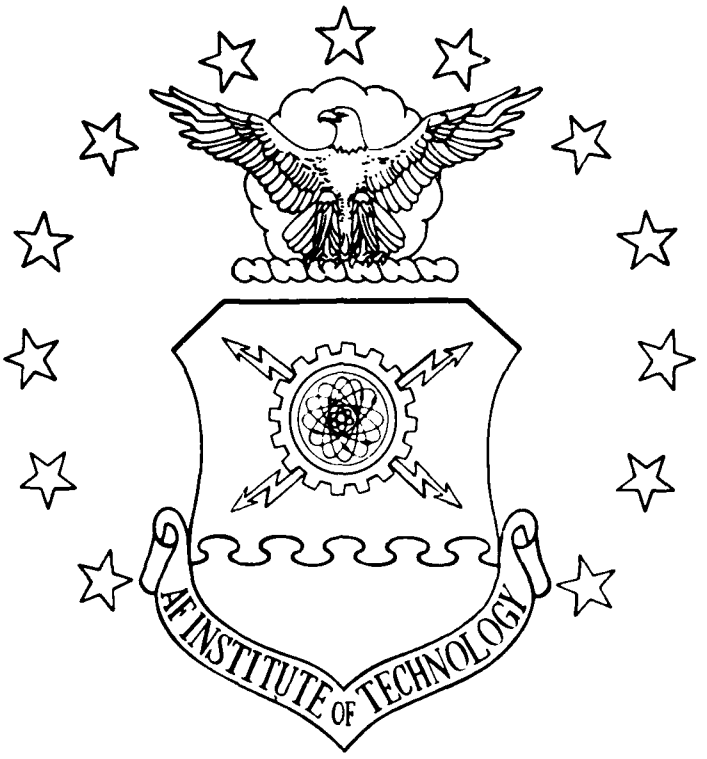


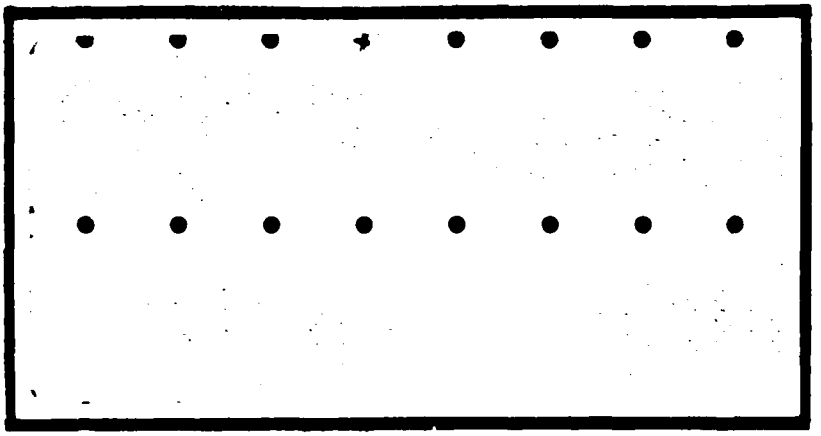


MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS-1963-A

(2)

AD-A161 332





DTIC FILE COPY

DTIC
ELECTE
NOV 21 1985
S D
E

DEPARTMENT OF THE AIR FORCE
AIR UNIVERSITY

AIR FORCE INSTITUTE OF TECHNOLOGY

Wright-Patterson Air Force Base, Ohio

This document has been approved for public release and sale; its distribution is unlimited.

85 11 18 109

2

AFIT/GLM/LSM/85

INTERFACING THE DEFENSE STANDARD AMMUNITION COMPUTER SYSTEM AND THE AIR FORCE COMBAT AMMUNITION SYSTEM: A SEARCH FOR AN ALTERNATE METHOD

THESIS

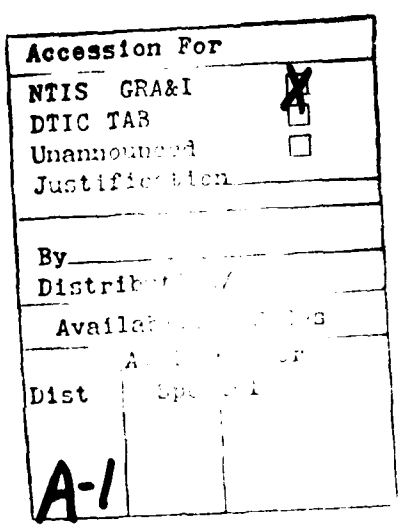
Alan C. Jones
Captain, USAF

AFIT/GLM/LSM/85S-39

Approved for public release; distribution unlimited

DTIC
ELECTE
NOV
S
D
E

The contents of the document are technically accurate, and no sensitive items, detrimental ideas, or deleterious information are contained therein. Furthermore, the views expressed in the document are those of the author(s) and do not necessarily reflect the views of the School of Systems and Logistics, the Air University, the United States Air Force, or the Department of Defense.



AFIT/GLM/LSM/85S-39

INTERFACING THE DEFENSE STANDARD AMMUNITION COMPUTER SYSTEM AND THE AIR FORCE COMBAT AMMUNITION SYSTEM: A SEARCH FOR AN ALTERNATE METHOD

THESIS

Presented to the Faculty of the School of Systems and Logistics

of the Air Force Institute of Technology

Air University

In Partial Fulfillment of the

Requirements for the Degree of

Master of Science in Logistics Management

Alan C. Jones, B.A.

Captain, USAF

September 1985

Approved for public release; distribution unlimited

Acknowledgments

In performing the research connected with this thesis effort I received a tremendous amount of help and guidance from others. I would like to thank all the individuals who willingly participated in my telephone survey. I would like to express my gratitude to my thesis advisor, Mr. Warren S. Barnes, for all the guidance received throughout this effort, and to my reader, Capt Rich Mabe, for his suggestions which helped me organize the presentation of my work. A note of thanks is in order to Mr. Tom Plante and Mr. Ralph McNamara from the Ogden Air Logistics Center, Directorate of Materiel Management, Airmunitions Requirements and Distribution Branch for sponsoring the research and helping me understand some of the wholesale aspects of munitions management. I would also like to thank Major Ian Birdsal and Fred Campbell at Headquarters AFLC who were patient enough to answer all my questions about the Combat Ammunition System and the World Wide Military Command and Control System. Finally, I would like to thank the members of my family, who understood the reason why we all had to sacrifice during the making of this thesis.

Alan C. Jones

Table of Contents

List of Figures

List of Tables

List of Acronyms

ACCAT	Advanced Command and Control Architectural Testbed
ACL	Access Control List
AF	U.S. Air Force
AFLC	Air Force Logistics Command
ALC	Air Logistics Center
AMCCOM	U.S. Army Armament and Chemical Command
AMPE	Automatic Message Processing Exchange
ARPANET	Advanced Research Projects Agency Network
AUTODIN	Automated Digital Network
AUTOSEVCOM	Automatic Secure Voice Communications
AUTOVON	Automated Voice Network
CAS	Combat Ammunition System
CSC	Computer Sciences Corp
CSC	DOD Computer Security Center
COMTEN	NCR Inc. Front End Processor
CPU	Central Processing Unit
DAA	Designated Approval Authority
DCA	Defense Communications Agency
DDN	Defense Data Network
DES	Data Encryption Standard
df	Degrees of Freedom
DISNET	DDN Integrated Secure Network
DOD	Department of Defense

DODIIS	DOD Intelligence Information System
DPS	Distributed Processing System
DSACS	Defense Standard Ammunition Computer System
E3	End-to-end-encryption
FORSCOM	U.S. Army Forces Command
FSM	FORSCOM Security Monitor
GAO	U.S. General Accounting Office
HQ	Headouarters
I-S/A	InterService/Agency
IBM	International Business Machines Inc.
IEEE 488	Institute of Electrical and Electronic Engineers Recommended Standard Protocol Number 488
IPLI	Internet Private Line Interface
KAIS	Korean Air Intelligence System
KG	Military-grade encryption device
LMI	Logistics Management Institute
LSI	Large Scale Integration
MILNET	Military Network
MINET	Movement Information Network
MRA & L	Manpower Resources Acquisition and Logistics
MMWD	Directorate of Materiel Managemment, Airmunitions Requirements and Distribution Branch
NASA	National Aeronautics and Space Administration
NAVELEX	Naval Electronics System Command
NCC	Network Control Center
NCR	National Cash Register Inc.
NSA	National Security Agency

OO-ALC	Ogden Air Logistics Center
OSD	Office of the Secretary of Defense
Rj	The sum of the ranks assigned to each alternative
RAP	Restricted Access Processor
RS232	Electronic Industrial Association Recommended Standard Number 232
SACDIN	Strategic Air Command Digital Network
SCOMP	Secure Communications Processor
SKIP	SCOMP Kernel Interface Package
STOP	SCOMP Trusted Operating Program
SMCA	Single Manager for Conventional Ammunition
SP	Sanitation Personnel
SPM	Security Protection Module
SWO	Security Watch Officer
TCB	Trusted Computer Base
TCP/IP	Transmission Control Protocol/Internet Protocol
Telnet	A General Telephone and Electric Corp Network Standard Virtual Terminal Protocol
TS	Top Secret
TSSO	Terminal System Security Officer
USAF	U.S. Air Force
VMIU	Virtual Memory Interface Unit
WIN	WWMCCS Intercomputer Network
WINCS	WWMCCS Intercomputer Network Communications Subsystem
WIS	WWMCCS Intercomputer System

WWMCCS	World Wide Military Command and Control System
X.25	Consultive Committe on International Telephone and Telegraph Public Data Network Recommended Standard Protocol Number 25 for Packet Switching

Abstract

Conventional ammunition management is becoming more centralized. The Army, as the Single Manager for Conventional Ammunition (SMCA), is developing the Defense Standard Ammunition Computer System (DSACS) to manage wholesale conventional inventories for all Military Departments. The unclassified DSACS is intended to interface with existing service ammunition systems. The Air Force is developing the Combat Ammunition System (CAS), a Secret system which will reside within the World Wide Military Command and Control System (WWMCCS) to manage Air Force wholesale and retail munitions worldwide. To be effective each system must exchange information on a real-time basis, however, a suitable interface has not been developed. This thesis used expert opinion to determine the best method of interface. A structured telephone survey was used to interview computer experts. The interview was designed to determine the necessary requirements for a suitable interface, to determine how well current technology could support the requirements, and to survey new developments in technology. Alternatives were ranked against six criteria and The Kendall Coefficient of Concordance (W) determined the

significance of the analysis. Conclusions were: (1) the major interface requirements must focus on computer security issues, (2) six fundamental security requirements must be met before an interface is considered "trusted" to link CAS and DSACS, (3) no current interface can provide a real-time interactive secure interface between CAS and DSACS, (4) the Secure Communications Processor (SCOMP) and the Restricted Access Processor (RAP) are two developing alternatives which best satisfied the criteria, (5) the analysis of alternatives was unable to choose which method was clearly the best. Recommendations were: (1) Air Force and Army should reevaluate their interface requirements for CAS and DSACS. (2) both services should initiate research in multilevel secure computer technology, (3) the RAP and SCOMP should be studied carefully by both services.

INTERFACING THE DEFENSE STANDARD AMMUNITION COMPUTER SYSTEM AND THE AIR FORCE COMBAT AMMUNITION SYSTEM: A SEARCH FOR AN ALTERNATE METHOD

I. Introduction

General Issue

In November 1975, Department of Defense Directive 5160.65 made the Army the Single Manager for Conventional Ammunition (SMCA). A major objective of the SMCA is to develop, design, and centrally maintain a standard DOD-wide automated data system as a high priority task critical to improving defense munitions management. The Army is developing the Defense Standard Ammunition Computer System (DSACS) to interface with existing service unique ammunition data systems (22). A suitable method to interface Air Force ammunition data systems with DSACS has not been developed.

Background

DSACS is the central data base system which the SMCA is developing that will manage wholesale conventional inventories for all the Military Departments. The Combat Ammunition System (CAS) is the Air Force data base system being developed to manage Air Force wholesale and retail

conventional ammunition assets worldwide. Retail assets are inventories which are stored at the base level, whereas wholesale assets are stored at the depot (10:22). Air Force conventional assets which can not be stored at base level are managed by the SMCA at various depots (22:5).

To be effective each system must be able to exchange information on a real-time basis. DSACS requires access to Air Force retail asset data from CAS in order to be able to determine total DOD requirements for each stock number. CAS requires the ability to access information from DSACS concerning wholesale asset status in order to maintain visibility over its total stockpile (45).

Justification for Research

The Joint Chiefs of Staff require timely and accurate information concerning the quantity, location, and condition of wholesale and retail conventional ammunition. Time-sensitive decisions concerning the allocation of ammunition during crises will be based upon the information provided by DSACS and CAS. The need for a real-time interactive interface between these two systems is critical to command and control decisions (43,46). This thesis represented an initial attempt to evaluate potential methods to interface DSACS and CAS.

Scope

The research was limited to single manager assigned conventional ammunition data of interest to the SMCA and the Air Force. Air Force wholesale and retail data is contained within the CAS, while wholesale data for all services is contained within DSACS (46). Functional objectives, performance objectives, and requirements discussed will be limited to the visibility of wholesale and retail assets, and the logistics data systems that support them. The computer interface will be between the Headquarters Air Force Logistics Command D078 (CAS) and DSACS, with special emphasis on Air Force computer systems.

Specific Problem

The current CAS munitions data base resides within the World Wide Military Command and Control System (WWMCCS), with a security classification of Top Secret. The DSACS data base will be unclassified, and will not be able to directly access the data it requires from CAS with an on-line interface because of the security classification of the CAS data base (64). A method to interface the two systems needed to be proposed and evaluated. In order to develop a proposal to solve the interface problem a number of investigative questions had to be answered.

Investigative Questions

1. What requirements will an interface method have to meet to be acceptable to both DSACS and CAS?
2. How well can current technology support these requirements?
3. What are the various interface methods currently in use?
4. What is the best method of interface?

Summary

This chapter has briefly described the general issue, background, justification and scope of the research, and has identified a specific problem regarding the development of two automated ammunition data systems. Specifically, a suitable interface has not yet been developed which will support real-time exchanges of data between the Army's DSACS and the Air Force's CAS. Four investigative questions were developed to provide a framework for the research and to provide the information necessary to develop an alternate method of interface. Chapter II will contain a historical perspective of conventional ammunition management during the past 45 years and will document the gradual trend towards centralized ammunition management.

II. Literature Review

Historical Perspective

Prior to 1939 the War Department did very little planning to prepare conventional munitions for a large conflict like World War II (66:116-117). In 1940 the War Department invested 3 billion dollars to build 100 ammunition production facilities which would have the capacity to produce about 15 billion dollars worth of ammunition per year by 1943 (12:2,40:81,65:193).

Responding to the needs of a peacetime economy following World War II, the nation reduced the number of production facilities from 100 to 60, and placed them in caretaker status. Post World War II policy was to respond to any future wars with a full mobilization of the private sector economy (12:2).

The outbreak of the Korean conflict forced the Department of Defense to return the 60 ammunition plants to full production. It was only after rehabilitation costs of 600 million dollars that these 60 plants were able to produce 7.5 billion dollars worth of ammunition for use in Korea (12:2). This heavy investment in the expansion of production capacity was largely supported by the private sector (65:193).

Because a huge excess of ammunition remained at the end

of the Korean hostilities, the nation virtually stopped production and reduced the number of production facilities to 30. Czapliki stated, "a few facilities were operated well below capacity" (12:3). Post Korean policy was to depend on private as well as government plants to deliver ammunition for future conflicts (65:201,66:43).

The reactivation of ammunition plants for the Vietnam build-up was costly and difficult because of the age of the facilities, the lack of automated techniques, and shortages of experienced personnel (44:34). In addition, the military services had been managing their ammunition inventories independently of each other (11:8). The Department of Defense did not maintain any official point of contact with the combined public and private industrial base (12:3).

The Secretary of Defense recognized the need for control over the fragmented service ammunition organizations and took action to provide centralized management. By 1965, under the centralized leadership of the Office of the Secretary of Defense (OSD), ammunition production reached 2.7 million tons per year. However, the centralized management of ammunition by the OSD was short-lived, and decentralized control returned to the services following the U.S. withdrawal from Vietnam (11:5,12:5).

As seen so far, the management of conventional ammunition from World War II until the end of the Vietnam

conflict followed a historical pattern. The pattern of ammunition production during these years was characterized by production gear-up during short periods of high demand followed by long periods of inactivity when demand was low (12:4,44:2).

Centralized Ammunition Management

Studies concerning centralized conventional ammunition began in 1968, when the Secretary of Defense requested an independent evaluation of the conventional ammunition production base (10:3). A Logistics Management Institute (LMI) Study, titled "Conditional Operation of DOD Ammunition Production Facilities", published in July 1970, studied both government and privately owned facilities. The report concluded that the start-up delays, inadequate capacity and costly operations experienced during Vietnam were a result of inadequate coordination of ammunition production (44:2). The Army had been scheduling production for critical munitions without knowing what schedules or production capacity the Navy was planning (12:5). The LMI study called for a centralized ammunition management system which would improve long-range planning and prevent costly plant start-ups and duplication of efforts among the services (12:5,44:75).

The General Accounting Office (GAO) Report, "Effective Central Control Could Improve DOD's Ammunition Logistics"

published in December 1973, recommended that the Secretary of Defense assign the responsibility of central management to a single service. The report suggested that central management would make better use of limited funds and production capacity by consolidating production schedules for all services (12:7,11:1-2).

Single Manager for Conventional Ammunition

On November 26, 1975, the Office of the Secretary of Defense (OSD) assigned to the Secretary of the Army the responsibilities of the Single Manager for Conventional Ammunition mission within the Department of Defense under DOD Directive 5160.65 (22:1). The objectives of the SMCA are to improve the efficiency and effectiveness of the ammunition acquisition process, eliminate overlap and duplication of effort among the Military Departments, and to maintain a strong production base for ammunition (22:1-2).

DOD Directive 5160.65 requires the SMCA to develop, design, and centrally maintain a standard DOD-wide automated wholesale data system. In February 1983 a joint service team recommended the networking of existing individual service systems as the best alternative to satisfying the requirement. This central system, when complete, will include all data files that impact the SMCA, and will be known as the Defense Standard Ammunition Computer System

(27:2-1).

The responsibilities and functions of the SMCA which are important to this research focus upon the wholesale supply functions and logistics data systems. The supply function requires the SMCA to maintain custodial accountability over Air Force wholesale assets and to report the quantity, location, and condition of these assets to the Air Force. The logistics data system which will be used is the Defense Standard Ammunition Computer System (22:5).

The Secretary of the Air Force also has supply and logistics data system responsibilities. The Air Force must provide the SMCA with the quantity, location, and condition of Air Force owned ammunition in stock which is common to more than one service. The information must be input into DSACS (22:10).

The major DSACS supply performance objective is to provide timely and accurate information concerning Air Force owned wholesale stockpiles in a manner which is compatible with the Combat Ammunition System (27:2-6,2-7).

Combat Ammunition System

The current Air Force Ammunition Reporting Management System (ARMS), originally developed in 1970, automated manual stock records to provide visibility for munitions inventories. Accounts at base level compile ammunition

transaction data, and transmit it to major commands who in-turn route data to a central data bank (See Figure 1). This system is known as the D078. As data is transmitted from major commands to the Air Staff it is often delayed by manual edit requirements resulting from existing program shortfalls. By the time inventory updates reach Air Staff they are nearly 60 days old (45).

In August 1982, the Air Force Deputy Chief of Staff for Logistics and Engineering directed that deficiencies in the D078 system be corrected (45). A major problem recognized was the lack of visibility over retail and wholesale ammunition (11:8). "Due to deficiencies in the current system there is a continuous imbalance in wholesale records maintained by the AF" (26:23). In January 31, 1983 the GAO reviewed the wholesale inventory asset record balances of the SMCA and the Air Force. They found 10.9 million dollars worth of overages at the SMCA and 21.3 million dollars worth of shortages on Air Force records (26:8). In response to these problems, the D078 was linked to the World Wide Military Command and Control System at Headquarters Air Force Logistics Command (HQ AFLC) (See Figure 2) (45). The D078 is now classified Top Secret because of its incorporation into the WWMCCS Honeywell Distributed Processing System (DPS-8) (45).

These changes in the D078 were in preparation for the

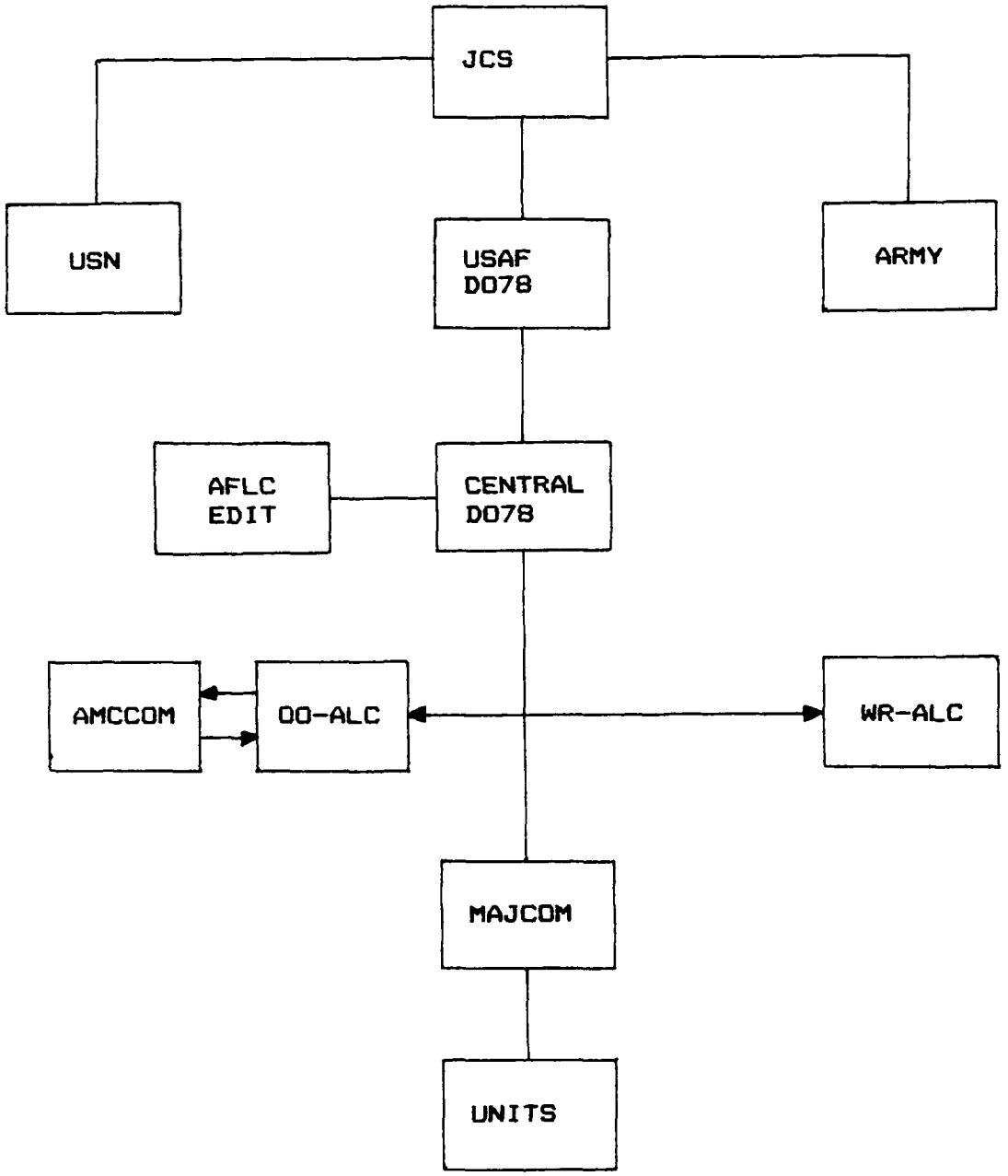


Figure 1. The D078 System (45)

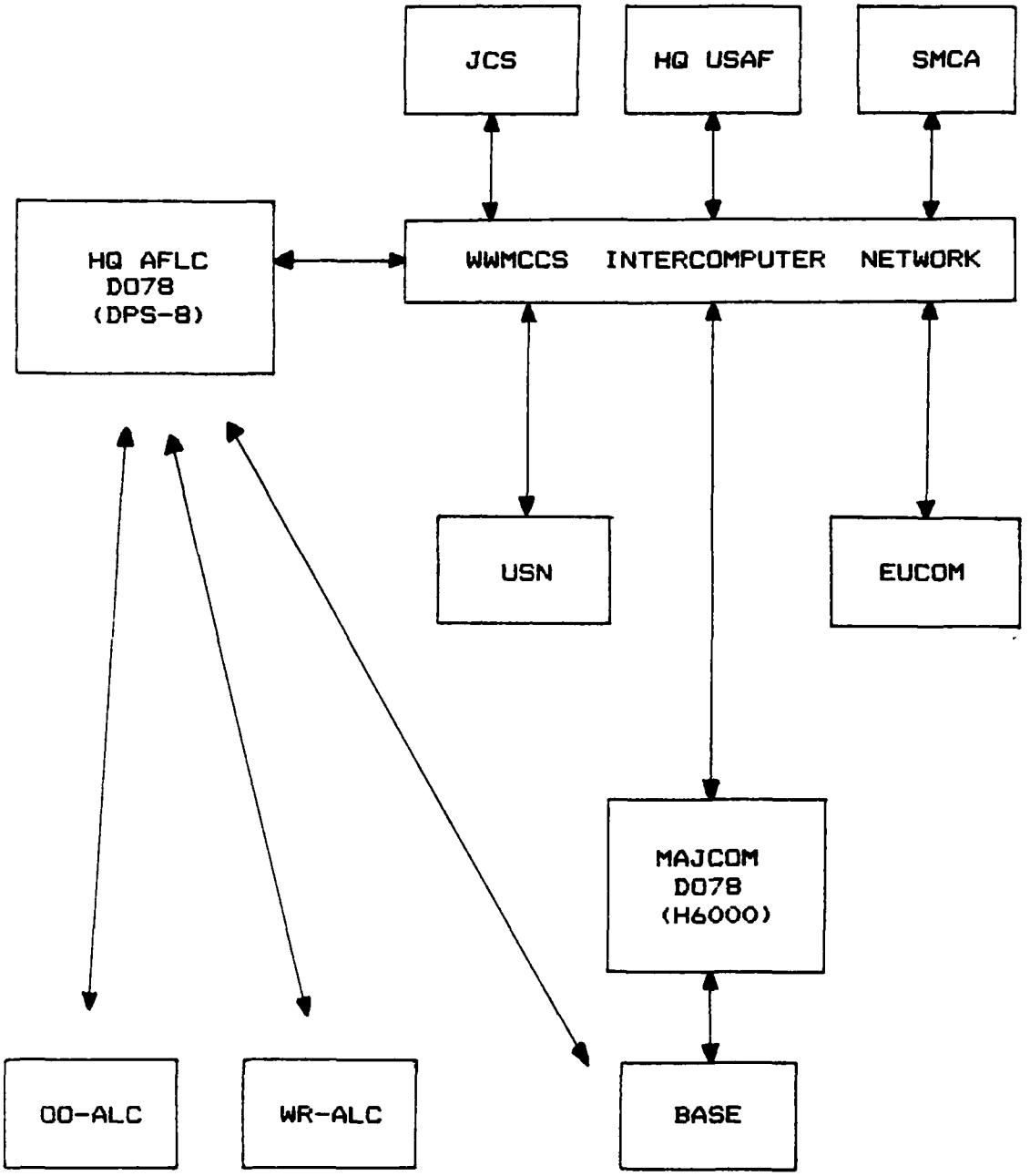


Figure 2. HQ AFLC Munitions Network (45)

Combat Ammunition System currently being developed by the Air Force. The CAS is designed to "be the only USAF system authorized for command, control, and management of munitions stocks worldwide." The future D078 will use WWMCCS and will be required to interface directly with DSACS (45).

Proposed Interim CAS-DSACS Interface

A conference was held in January 1985 between the Army and Air Force to discuss the problem of interfacing CAS and DSACS. An interim method was worked out for an interface which may have some temporary utility. (See Figure 3). The Air Force Honeywell 8000 can download retail asset data to a Honeywell Front-End Processor (H716) which has an interface with the Automatic Digital Network (AUTODIN). The Army recently received a National Cash Register Corporation (NCR) Front-End Processor (COMTEN) which will have interface capability with AUTODIN and the Army's International Business Machines Corporation (IBM) 4341 System. The SMCA will be able to send wholesale asset data via COMTEN and AUTODIN to the H716. Both services recognize this possible interface as a temporary and interim method and not as an acceptable solution to the problem (42). The most obvious problem with this type of interface is the fact that both DSACS and CAS can only push data towards each other, but neither system has the ability to pull data from the other.

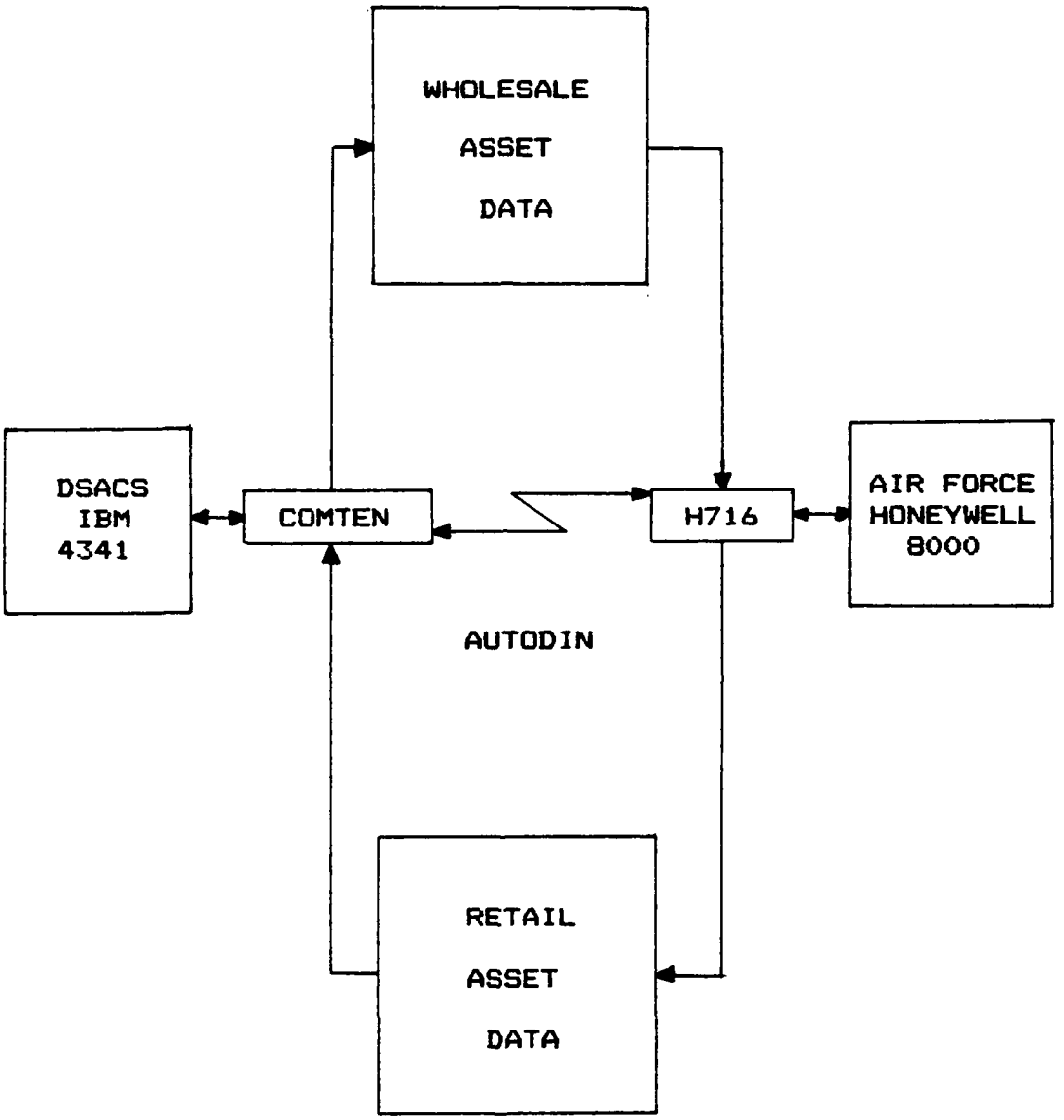


Figure 3. Proposed CAS-DSACS Interface (42)

Summary

This chapter began with a historical perspective of the past 45 years of conventional ammunition management and followed with a documentation of studies urging the DOD to accept a centralized ammunition management concept. The chapter further covered the SMCA assignment to the Army and the subsequent development of the Defense Standard Ammunition Computer System and the Air Force's Combat Ammunition System. Chapter III will describe the method by which a proposal for a suitable interface between DSACS and CAS will be developed.

III. Methodology

Introduction

The literature review has documented Department of Defense efforts to solve problems encountered in the management of conventional munitions since World War II. These efforts have lead to the establishment of the Defense Standard Ammunition Computer System and the Combat Ammunition System (12,22,27,45). Together, these two systems have the potential for allowing the Joint Chiefs of Staff and the Air Staff to have real-time data at their fingertips when making command and control decisions. However, the Army and the Air Force developed their respective ammunition computer systems independently of each other. There was no common plan for an interface between DSACS and CAS (45). The lack of a suitable interface is preventing the realization of the systems' full potential. This chapter presents the research design used to develop the best alternate method of interface.

Overview of the Research Effort

Emory defines research as an "inquiry carried out to secure information for solving problems" (30:8). The objective of this research was to collect, analyze, and evaluate information gathered from computer experts about the

alternate methods of interfacing DSACS and CAS. The purpose of the research was to develop a number of plausible interface alternatives and recommendations to be presented to the Army and Air Force.

The first step of the research was to define what information was required to solve the problem. In order to develop proposals for the best interface between DSACS and CAS, four investigative questions had to be answered.

1. What requirements will an interface method have to meet to be acceptable to both DSACS and CAS?

2. How well can current technology support these requirements?

3. What are the various interface methods currently in use?

4. What is the best method of interface?

The aforementioned investigative questions were answered through the use of seven interview questions (Appendix A). The next step was to determine where the required information could be found. The research focused upon a population of computer experts in government and private business for this information (Appendix B). A sample of computer experts had to be found which would be familiar with the Air Force hardware and software involved and/or familiar with the newest developments in the computer industry. A valid and practical research instrument had be developed to gather the information from the experts to answer the four investigative

questions. A structured telephone interview was used for this purpose.

The first investigative question was designed to determine what requirements were necessary to satisfy the needs of CAS and DSACS. Therefore it was restated as the first interview question. The second and third investigative questions were designed to determine if current technology could support these interface requirements and whether or not such technology existed today. Interview questions two, three, four, five and six were designed to make an assessment of the current state of technology. The seventh interview question was designed to encourage comments on what areas the Air Force should concentrate on to solve the interface problem.

The experts needed a guide which would help them limit their responses to the interview questions. A set of functional requirements was developed by Ogden Air Logistics Center, Directorate of Materiel Management, Airmunitions Requirements and Distribution Branch (OO-ALC/MMWD) and Headquarters Army Armament Munitions and Chemical Command (HQ AMCCOM). They identified the requirements a suitable CAS/DSACS interface method must meet (43,46). Their requirements were included as part of a standard letter which was sent to all the computer experts prior to the telephone interview (Appendix A).

Finally, a decision rule had to be established to determine which interface method was the best one to recommend to the Army and the Air Force. The decision rule will be fully explained in a later section in this thesis.

Definition of the Population

The population was defined as scientific and computer analysts from the Air Force Logistics Management Center, Air Force Data Systems Design Center, the Pentagon, Headquarters Air Force Logistics Command/Logistics Operations Center, the Air Force Electronic Systems Division, Synergy Inc., Omnicom Inc., Honeywell Inc., NCR COMTEN Inc., Computer Sciences Corp., Headquarters Defense Communications Agency, MITRE Corp., Cincom Systems Inc., Savings and Loans Data Corp., Verdix Corp., Logicon Inc., DOD Computer Security Center. This population included military personnel, federal employees and private sector civilians who either had specific knowledge about Air Force computer systems or were knowledgeable about the latest developments in the computer industry. Once the population was defined, the method of selection of the survey sample needed to be determined.

Selection of the Sample

The population of computer experts defined was much too large and dispersed to be contacted through a census. Therefore, a sample of the population was taken because of the following advantages.

1. The characteristics of the defined population can be determined in a much shorter time through sampling rather than through a census.

2. Sampling reduces the cost of a survey.

3. Administratively, a total canvass effort is often extremely difficult, if not impossible to accomplish with limited time and money.

4. More attention can be devoted to each individual contacted when a reasonable size sample is chosen (49:109-110).

The decision to select a survey sample was not made without regard to some inherent disadvantages.

1. Sources of error can be introduced and the results of the survey could be misleading if the sampling procedure is not well designed and followed.

2. Depending on the size of the population, a small sample may not accurately represent the population.

3. Screening techniques used to find a sample of a population with specific characteristics takes a lot of time and, depending on the length of the screening interview and the number of call backs required, can be expensive (61:40).

Before it was decided what type of sample to use, various sampling methods were reviewed. The sampling methods reviewed were random sampling, stratified sampling, and

nonprobability sampling.

Random sampling is a method by which each member of the population has an equal chance of being selected. However, one of the requirements of this method is that the sampling units selected be independent of each other (49:219-225). For the purpose of this research it was necessary to screen potential respondents and build a list of experts who possessed specific experience and knowledge of computer systems. The process of personal referral was used extensively to develop the sample of experts. A random selection of individuals would not have been appropriate for this objective.

A stratified sampling method involves classifying the population into two or more classes and making a random selection from within each stratum (49:226). The proportion of civilians versus military personnel possessing specific computer experience in the population is not known. Furthermore, it is the gathering of a sum total of information available from all individuals in the sample which was the objective of the data collection. No further purpose would be served if the population were stratified. In this case the stratified sample would only be as good as a random sample (49:228).

The nonprobability sampling method is used when it is not desireable or feasible to choose from a population in a

purely random fashion (30:177,49:237). The sample of computer experts for this thesis was chosen using a nonprobability method. It is a more appropriate method when the objectives of the research are limited and when the researcher "may be looking only for a feel of the range of the conditions, or for examples of dramatic variations" (30:177).

There are two methods of nonprobability sampling: one for convenience, and one which is purposive. The convenience method would imply that the sample be chosen by selecting those individuals who were the first ones to be found and were the easiest to interview. There are no prerequisites for choosing a sample by convenience. On the other hand, purposive methods of sample selection "involve a more delibrate effort to secure a sample that conforms to some predetermined criteria" (30:177,49:236-237).

There are two varieties of purposive sampling: expert choice and quota sample. The quota sample is used most often to build a sample which has the same characteristics as the population in the same proportion as they occur in the population. For example, if a population was believed to be 60 percent Catholic and 40 percent Protestant, the sample would be selected so that the quota of 60 percent Catholic and 40 percent Protestant was satisfied.

Nonprobability sampling by expert choice is "most useful in studying those cases which we believe are in the best

position to provide us with information" (30:178). The computer experts chosen for this research had to be knowledgeable about Air Force computer systems and/or the latest developments in the computer industry, and were the only persons who could have provided the necessary information.

This thesis used expert choice sampling. The selection process was primarily initiated by referrals, whereby experts were referred to the researcher by their peers based upon a knowledge of their specialized background. Other experts were found by contacting the functional offices of computer companies and consulting firms. Each potential respondent was initially contacted by the researcher on the telephone and a screening interview was conducted. The general issue, background information, and the specific problem of the thesis effort were discussed with the potential respondent. The potential respondent was asked to comment on how his or her particular experience could be applied to the search for an alternate method of interface. If the potential respondent felt capable of answering the interview questions and expressed an interest to participate in the thesis effort the researcher invited him or her to participate in the telephone interview. Only those potential respondents who agreed to participate in the interview were included in the sample population.

Structured Telephone Interview

Once the sample of computer experts had been found and had agreed to participate in the research effort, a method of securing information had to be developed. The three most frequently used data collection techniques are mail surveys, telephone surveys and personnel interview surveys (49:331). The selection of a particular survey method should be based on the cheapest method available that can provide the required information (60:279). A structured telephone interview technique was designed to incorporate some of the advantages of the mail survey with those of the telephone survey and to avoid some of the disadvantages of telephone and personal interviewing.

Advantages. The telephone interview was chosen because of some very significant advantages.

1. The telephone is a convenient way to secure information from respondents who are spread out over a large geographical area, because it eliminates the time and cost of travel (61:66-67).

2. The interview questions can easily be standardized (49:91).

3. "The cost per completed interview is low for the sample covered" (49:91).

4. Professionals and businessmen are well accustomed to and are dependent upon the telephone as a means of communication. They are much more accessible for interviews over the telephone than by face-to-face interviews (61:65).

5. When compared to mail surveys the telephone survey has a higher participation rate on the initial contact (49:92).

6. Often the quality of the information gathered by the telephone survey is higher than when face-to-face interviews are used because the interviewer is more at ease working within familiar surroundings and the respondent "is more candid than he would be in a face-to-face interview" (30:306,61:58).

7. When it is necessary to screen a population to find sufficient cases to build a sample for analysis, the cooperation rate can be as least as good as achieved by face-to-face methods, and at about one third of the cost (61:63-67).

Disadvantages. The structured telephone interview was not selected until after its most significant disadvantages were reviewed.

1. Respondents may not react favorably when asked to answer questions over the telephone that require detailed information or that take up too much of their time (49:92,60:263).

2. A respondent may not feel compelled to amplify his replies over the telephone and the interviewer may not have enough time to write down all of the response.

3. The interviewer is subject to the unavailability of the respondent because of busy signals, no answer, or time spent away from the office.

4. The timing of the telephone call may affect the respondent's attitude and willingness to answer questions. The interviewer will not normally be aware of meetings and appointments scheduled by the respondent (49:93).

5. The appropriate length of an interview is dependent on the amount of interest the respondent has for the subject matter (30:307).

6. Telephone interviews should not require extensive use of visual aids or complex charts or graphs. Questions should be kept simple.

7. It is much easier for the respondent to terminate a telephone interview than it is to terminate a personal interview (30:307).

Justification. In order to minimize the unfavorable reaction of some respondents when asked questions that require considerable thought and preparation to answer, a standard set of questions was developed and mailed to the respondent well ahead of the telephone interview date. When mail procedure is combined with the telephone interview in this manner it is possible to answer open-ended questions and to avoid some of the disadvantages of mail surveys (60:272). By the time of the interview, the respondent had had ample time to consult with others, gather data, and formulate answers to the questions. The opportunity for advanced preparation should also have increased the willingness of the respondent to amplify his responses (60:151-152,263).

The ability of the interviewer to write down the responses during the interview was enhanced by the use of a tape recorder to record the responses to all interview questions. During the screening interview the researcher requested the permission of each respondent to allow a tape recording of the forthcoming interview. No interviews were tape recorded without the permission of the respondent. The initial screening of the respondents helped to insure that the participants were well qualified, would have a high

degree of interest in the topic and would be willing to take the time necessary to prepare for and respond to the interview questions (60:272).

The structured telephone interview is an efficient and cost effective method of securing information (49:91). The intitial screening of potential respondents, the forwarding of standardized questions to the participants ahead of time and the tape recording of the responses helped overcome some of the inherent disadvantages of the telephone survey. Once the structured telephone interview technique was chosen the response format had to be determined.

Response Format. According to Kahn and Cannel, there are five factors which need to be determined before the degree of structure in the response should be determined.

1. Objectives of the interview
2. Respondents' level of information
3. Respondents' level of preparation
4. Willingness of the respondent to discuss the topic
5. Degree to which these factors are known by the interviewer (30:234).

There are two major categories of response formats: open-answer and closed-answer. The closed-answer response is one in which the respondent is limited to specific responses from which one or more may be selected (60:152). An open-answer response format is one in which the respondent answers a question in his or her own words and the response is taken by the interviewer exactly as it is given. The

open-answer format encourages the respondent to introduce their own opinion in a manner which is most comfortable for them. "It is an absolutely essential tool when you are beginning work in an area, and need to explore all aspects of the opinion area"(60:150-151).

The objective of the interview conducted for this thesis was to gather information which may lead to a better interface between DSACS and CAS. This objective required that the respondents express their knowledge and opinions freely. The open-ended question is well suited to an interview which may require some additional questions and comments to clarify the issue. The open-ended question is appropriate when the interviewer is not sure of the frame of reference and level of knowledge of all the respondents (30:234). Although all respondents were considered to be experts, they each had a unique frame of reference which depended on their experiences within the computer industry. An open-ended question is appropriate when the respondent would benefit by having a chance to think over the question and to be able to revise it before the final response is taken (30:234). Thus, the open-ended question best served the purposes of this research.

Data Collection

A standard letter was prepared and sent to each participant in advance of the telephone interview (Appendix A). The letter contained an introduction to the research effort and included a brief description of the general issue and the specific problem, as well as the interview questions. Approximately seven to ten days was allowed for the letter to arrive and for the respondents to formulate their thoughts. After this time the telephone interview was conducted and all those respondents who consented to a tape recording had their responses recorded. Once all the responses were recorded, it was necessary to develop a decision rule to analyze the various alternatives and to determine which solutions were the best.

Decision Rule

This section describes the technique by which the best alternative interface method was chosen.

Decision Process. The decision process consists of defining the problem, identifying the alternatives, quantifying the alternatives, applying decision aids, making the decision and implementing the decision (2:22). The research problem was identified in Chapter I: a suitable method of interface between CAS and DSACS had to be proposed

and evaluated. A literature search was completed and it was found that, indeed, there was no suitable interface method being used and that it was a problem worth solving. The next step in the decision making process was to identify the alternatives. The alternative choices were not readily apparent at the onset of the research. Therefore, a structured telephone interview was conducted to gather information from a sample of computer experts. The alternatives were drawn from the information collected during the interviews. The next step in the process was to develop a decision matrix which would quantify the alternatives and facilitate making a logical decision.

Decision Matrix. A decision matrix was developed to show the rank order of the alternatives with respect to the degree to which they satisfied a number of selection criteria. Every alternative was ranked on an ordinal scale to show its relationship to other alternatives when judged individually against each of six selection criteria (See Figure 4). Selection criteria chosen by the researcher were:

1. Time to implement the alternative interface method.

2. Interoperability of the CAS and DSACS systems allowed by the alternative method.

3. Security. The ability of the method to protect classified information from being accessed by unauthorized users of the two systems.

4. Expandability. The potential for the

alternative method to be incorporated into a larger network of computer systems at a later date.

5. Permanence. The possibility that the alternative represents a permanent solution.

6. Real Time. The relative speed of processing and transmitting information between CAS and DSACS.

Time criteria was selected as an important factor to consider when evaluating the alternatives. On 15 October 1982 the Assistant Secretary of Defense for Manpower Resources Acquisition and Logistics (MRA&L) declared the development of DSACS critical to improving defense munitions management and wanted the program accelerated as a high priority task (16). Obviously the timely implementation of an acceptable solution would be preferred to one which would take a long time (more than 5 years) to implement. Interoperability was chosen as an important selection criterion because the Air Force desires a standard on-line interactive system between the SMCA and all Services (27:4-3,16). Security of the two systems was chosen as an important selection criterion because the DOD concept for DSACS and CAS development requires all interfacing systems to provide for protection of both classified and unclassified data (27:4-2,46). Expandability was chosen as an important selection criterion because DSACS must use the most current technologies and be able to incorporate advancements as they occur (27:4-1). The possibility of the alternative

representing a permanent solution to the interface problem was chosen as an important selection criterion by the researcher because of the enormous cost associated with the acquisition of major systems. The implementation of an interim interface method would be expensive and may not represent a large enough improvement to warrant the cost. The ability of the two systems to interact in a real-time manner was chosen as an important selection criterion because this requirement has been expressed by both the Army and the Air Force (43,46).

	Alternative			
	A1	A2	A3	A4
Time	1	2	3	4
Interoperability	4	3	2	1
Security	1	4	2	3
Expandability	2	3	4	1
Permanence	1	2	4	3
Real Time	2	1	3	4
Rj	11	15	18	16

Rj - The sum of the rank for each alternative.

Figure 4. Example of Decision Matrix (56:230)

See Appendix C for a more detailed explanation about how each alternative will be chosen and ranked against these criteria by the researcher. Once the relationships between all alternatives and the selection criteria had been established, the Kendall Coefficient of Concordance (W) was computed to determine the degree of the agreement among the rankings.

Kendall Coefficient of Concordance: (W). The Kendall Coefficient of Concordance is a nonparametric statistic which measures the correlation between k sets of selection criteria ranking N alternatives. The W statistic is best suited for ordinal or nominal data when no assumptions are made about the shape of the population from which the scores were drawn. Once rank order of alternatives are determined for each selection criteria the W statistic can be computed. When observations result in a tied ranking, the average of the ranks that would have been assigned if no tie had occurred are assigned (56:196).

Method. Reference Figure 4.

1. Let N = 4, the number of alternatives to be ranked and let k = 6, the number of selection criteria. Put the rankings in a k x N table.

2. For each alternative, determine Rj, the sum of the ranks assigned by the k selection criteria. Rj = 60.

3. Find the mean of the Rj ($\bar{R}j$). Express each Rj as a deviation from that mean, square the deviation and sum the deviations to get s.

$$\bar{R}j = Rj/N = 60/6 = 10 \quad (1)$$

$$s = \Sigma(\bar{R}j - Rj)^2 \quad (2)$$

$$s = (10-11)^2 + (10-15)^2 + (10-18)^2 + (10-16)^2$$

$$s = 126$$

4. If the proportion of ties in the k sets of ranks is large use the formula:

$$W = \frac{s}{.083k^2 (N^3 - N) - k \Sigma T} \quad (3)$$

Where $$T = \frac{\Sigma(t^3 - t)}{12} \quad (4)$$

to compute W. If the proportion of ties is small use:

$$W = \frac{s}{.083k^2 (N^3 - N)} \quad (5)$$

$$W = \frac{126}{(.083)(36)(60)} = .70$$

to determine W.

5. In order to test the W for significance, test the hypothesis that the k sets of rankings are independent. The alternative hypothesis is that the k sets of rankings are related.

a. For N less than 7, Table I has critical values for s associated with W, significant at the .05 and .01 levels. If the observed s is greater than or equal to the critical value of s for k,N, then the original hypothesis is rejected and the W is significant.

W = .70 s = 126

s observed > s critical

126 > 75.5 at .05 level of significance.

b. For N greater than 7, use the formulas:

$$df = N-1 = \text{degrees of freedom} \quad (6)$$

$$X = k(N-1)W \quad (7)$$

c. If X is greater than the value in Table II for a certain level of significance and degree of freedom, then the agreement among the selection criteria is higher than it would be by pure chance (56:229-239).

Interpretation. A high or significant value of W does not necessarily mean that the rank orders are correct. It does support, however, whether or not the ranked judgements were made in agreement among the selection criteria. "Kendall suggests that the best estimate of the "true" ranking of N objects is provided when W is significant, by the order of the various sums of ranks, Rj". Therefore, in Figure 4 alternative A1 is the best with Rj = 11, followed by alternatives A2, A4 and A3 (56:238).

Summary

This chapter explained the methodology which was used to answer the investigative questions. The population was defined, the sample population was selected and the data collection instrument was chosen and justified. Finally a decision rule and matrix was chosen and a step by step process was offered to explain how the best alternative interface method would be selected. The next chapter will contain the analysis of the research findings.

Table I

Critical Values of s in the Kendall Coefficient of Concordance

k	N					Additional Values for N = 3	
	3	4	5	6	7	k	s
	Values at the .05 level of significance						
3			64.4	103.9	157.3	9	54.0
4		49.5	88.4	143.3	217.0	12	71.9
5		62.6	112.3	182.4	276.2	14	83.8
6		75.7	136.1	221.4	335.2	16	95.8
8	48.1	101.7	183.7	299.0	453.1	18	107.7
10	60.0	127.8	231.2	376.7	571.0		
15	89.8	192.9	349.8	570.5	864.9		
20	119.7	258.0	468.5	764.4	1,158.7		
	Values at the .01 level of significance						
3			75.6	122.8	185.6	9	75.9
4		61.4	109.3	176.2	265.0	12	103.5
5		80.5	142.8	229.4	343.8	14	121.9
6		99.5	176.1	282.4	422.6	16	140.2
8	66.8	137.4	242.7	388.3	579.9	18	158.6
10	85.1	175.3	309.1	494.0	737.0		
15	131.0	269.8	475.2	758.2	1,129.5		
20	177.0	364.2	641.2	1,022.2	1,521.9		

Source: (56:286)

Table II

Critical Values of Chi Square

Probability that X is greater than or equal to chi square

df	.99	.98	.95	.90	.80	.70	.50
1	.00016	.00063	.0039	.016	.064	.15	.46
2	.02	.04	.10	.21	.45	.71	1.39
3	.12	.18	.35	.58	1.00	1.42	2.37
4	.30	.43	.71	1.06	1.65	2.20	3.36
5	.55	.75	1.14	1.61	2.34	3.00	4.35
6	.87	1.13	1.64	2.20	3.07	3.83	5.35
7	1.24	1.56	2.17	2.83	3.82	4.67	6.35
8	1.65	2.03	2.73	3.49	4.59	5.53	7.34
9	2.09	2.53	3.32	4.17	5.38	6.39	8.34
10	2.56	3.06	3.94	4.86	6.18	7.27	9.34
11	3.05	3.61	4.58	5.58	6.99	8.15	10.34
12	3.57	4.18	5.23	6.30	7.81	9.03	11.34
13	4.11	4.76	5.89	7.04	8.63	9.93	12.34
14	4.66	5.37	6.57	7.79	9.47	10.82	13.34
15	5.23	5.98	7.26	8.55	10.31	11.72	14.34
16	5.81	6.61	7.96	9.31	11.15	12.62	15.34
17	6.41	7.26	8.67	10.08	12.00	13.53	16.34
18	7.02	7.91	9.39	10.86	12.86	14.44	17.34
19	7.63	8.57	10.12	11.65	13.72	15.35	18.34

Source: (56:249)

IV. Findings and Analysis

Introduction

This chapter will present the findings of the thesis and will provide an analysis of the findings. The chapter is divided into seven subheadings. The first subheading will contain the results of the telephone interviews. The second and third subheadings, respectively, will identify the findings, and justify the selection of a number of alternatives which were offered by the computer experts as possible solutions to the CAS-DSACS interface problem. (See Appendix C). The fourth subheading will provide an analysis of the alternatives using the decision-making methodology described in Chapter III. Every alternative will be rank ordered against each of six criteria established by the researcher and described in Appendix C. The fifth subheading will describe how the Kendall Coefficient of Concordance was applied to the data which resulted from the rank ordering of the alternatives. The sixth subheading will contain a test of the significance of the resulting Kendall Coefficient of Concordance. The final subheading will provide a summary of the chapter.

Results

Each participant of the structured telephone interview received a questionnaire package in the mail prior to their interview, because they needed a guide which would help them limit their responses to the interview questions. (See Appendix A). Each individual was allowed at least one week to look over the package and formulate a response to the interview questions. The participants were requested to formulate their responses only after considering four interface requirements which were identified by the Army and Air Force specifically for the CAS-DSACS interface (43,46). These interface requirements were included as part of the questionnaire package. (See Appendix A). The results of the interviews will be provided in the order of the questions asked during the interview.

Interview Question 1. The responses to the first interview question highlighted some reservations about the ability of any commercial vendor to provide a real-time secure interface between DSACS and CAS. Twenty-six respondents believed that commercial vendors could not support the requirement to build a real-time secure interface as long as the two systems maintained different levels of security on their data.

These respondents generally believed that "real time" could be defined as a negligible period between the moment

data is transmitted by one system and received by another system, or an almost instantaneous transmission. However, three respondents believed the DSACS and CAS developers should define their concept of real time before they define the interface requirements needed to support the concept (28,31,67). These same three respondents were very skeptical about the need for an instantaneous exchange of data between CAS and DSACS. One respondent felt that the requirement for real-time interaction should be dropped entirely (64). Two respondents commented that the DSACS and CAS design engineers need to establish an open dialogue on the definition of terms and system requirements while each system is still in the development stage (28,32).

A number of respondents made positive comments on the potential for an interface method to support real-time interaction. Two respondents cited a developing effort being designed to address the problem of real-time interaction between a classified data base and various unclassified data bases (55,59). The development is called The Restricted Access Processor (RAP). Appendix I contains a description of RAP.

In addition to the two supporters of the RAP development, there were three respondents who believed that commercial vendors could support real-time interaction betweer DSACS and CAS (32,33,38). However, according to

these respondents, in order to accomplish this interface, a vendor would have to require DSACS and CAS to operate at the same level of security. This mode of operation is known as a system high mode. A description of a system high mode and other modes of operation (controlled mode, dedicated mode, and multilevel secure mode) can be found in Appendix M.

The majority of the respondents felt that the major requirements necessary to interface CAS and DSACS would not revolve around the issue of real time, but instead, would focus on the security issue of linking the unclassified DSACS to the Top Secret CAS (5,6,14,28,31,33,35,37,38,41,47,48,53, 55,57,58,67). Nine respondents felt that a security filter would be necessary between the two systems to insure unclassified data transmitted from CAS to DSACS would not contain any classified data (1,13,14,29,41,50,57,58,64). At least seven respondents made a direct mention of the "Orange Book" as one of the "absolutely essential references" containing the security requirements necessary to interface CAS and DSACS (6,37,48,50,53,55,64).

The Orange Book. The "Orange Book" is formally known as the Department of Defense Trusted Computer System Evaluation Criteria, CSC-STD-001-83, published by the DOD Computer Security Center. The major goal of the Computer Security Center "is to encourage the widespread availability of trusted computer systems for use by those who process

classified or other sensitive information" (19:1). The purpose of the Orange Book is threefold:

> -To provide users with a metric with which to evaluate the degree of trust that can be placed in computer systems for the secure processing of classified and other sensitive information.
>
> -To provide guidance to manufacturers as to what security features to build into their new and planned, commercial products in order to provide widely available systems that satisfy trust requirements for sensitive applications.
>
> -To provide a basis for specifying security requirements in acquisition specifications (19:2).

The Orange Book addresses the development of a statement of requirements for computer security, by describing a number of requirements necessary to define a computer system as "secure" (19:3). A secure system should have fully developed security features which will control access to information. Only authorized individuals and/or processes should read, write, create, or delete responsibilities for certain types of data. Six fundamental computer security requirements cover the need to control access to information and the need to prove that such control is actually being accomplished (19:3).

Fundamental Computer Security Requirements. Six fundamental computer requirements deal with the security policy, the accountability, and the assurance measures necessary for a computer system to become trusted.

Policy

Requirement 1 - SECURITY POLICY - There must be a well defined security policy enforced by the system. Given identified subjects [users] and objects [data elements], there must be a set of rules that are used by the system to determine whether a given subject can be permitted to gain access to a specific object (19:3,29,55).

Requirement 2 - MARKING - Access control labels must be associated with objects. In order to control access to information stored in a computer, according to the rules of a mandatory security policy, it must be possible to mark every object with a label that reliably identifies the object's sensitivity level (e.g. classification), and/or the modes of access accorded those subjects who may potentially access the object (19:3,31,55).

Accountability

Requirement 3 - INDENTIFICATION - Individual subjects must be identified. Each access to information must be mediated based on who is accessing the information and what classes of information they are authorized to deal with. This identification must be securely maintained by the computer system and be associated with every active element that performs some security-relevant action in the system (19:3,29,31,37,50,55).

Requirement 4 - ACCOUNTABILITY - Audit information must be selectively kept and protected so that actions affecting security can be traced to the responsible party (19:3).

Assurance

Requirement 5 - ASSURANCE - The computer system must contain hardware/software mechanisms that can be independently evaluated to provide sufficient assurance that the system enforces requirements 1

through 4 above. ...These mechanisms are typically embedded in the operating system and are designed to carry out the assigned tasks in a secure manner. The basis for trusting such system mechanisms in their operational setting must be clearly documented such that it is possible to independently examine the evidence to evaluate their sufficiency (19:3,37,55).

Requirement 6 - CONTINUOUS PROTECTION - The trusted mechanisms that enforce these basic requirements must be continuously protected against tampering and/or unauthorized changes. No computer can be considered truly secure if the basic hardware and software mechanisms that enforce the security policy are themselves subject to unauthorized modification or subversion (19:3).

The above six requirements form the foundation upon which the DOD Computer Security Center bases a set of criteria used to evaluate computer systems. There are four major divisions of criteria (19:5).

The Structure of the Criteria.

The criteria are divided into four divisions: D,C,B, and A, ordered in a hierarchical manner with the highest division (A) being reserved for systems providing the most comprehensive security (19:5).

Division D: Minimal Protection. This division contains only one class. It is reserved for those systems that have been evaluated but fail to meet the requirements for a higher evaluation class (19:9).

Division C: Discretionary Protection. Classes in this division provide for discretionary (need-to-know) protection, and through the inclusion of audit capabilities, for accountability of subjects and the actions they initiate (19:11).

> Division B: Mandatory Protection. The notion of a [trusted computing base] TCB that preserves the integrity of sensitivity labels and uses them to enforce a set of mandatory access control rules is a major requirement in this division. Systems in this division must carry the sensitivity labels with major data structures in the system. The system developer also provides the security policy model on which the TCB is based and furnishes a specification of the TCB. Evidence must be provided to demonstrate that the reference monitor concept has been implemented (19:19).

> Division A: Verified Protection. This division is characterized by the use of formal security verification methods to assure that the mandatory and discretionary security controls employed in the system can effectively protect the classified and other sensitive information stored or processed by the system. Extensive documentation is required to demonstrate that the TCB meets the security requirements in all aspects of design, development, and implementation (19:41).

These criteria are to be applied in conjunction with the fundamental computer security requirements "by system managers in selecting and specifying systems that have sufficient security protection for specific operational environments" (17:1-2). According to the Computer Security Center, linking an unclassified data base to a Top Secret data base requires the verified protection afforded only by a criteria class A1 certification (17:8-10). A more detailed description of all the classes within each criteria division can be found in Appendix L.

Interview Question 2. The respondents made it clear that there are a number of current interface methods which can support the secure transmission of classified data between two computer systems. Automatic Digital Network (AUTODIN), Automated Secure Voice Communications (AUTOSEVCOM), Defense Data Network (DDN), Defense Data Network Integrated Secure Network (DISNET), and Worldwide Military Command and Control System Intercomputer Network (WIN) were current communications systems cited as capable of supporting classified transmission of data (3,6,13,28,33,38,41,47,54). However, one common deficiency cited against all of these communications systems is the fact that each are required to operate in a system high mode between the sender and receiver of data. A system high mode of operation would require DSACS and CAS to operate at the same level of security. Twenty-two of the twenty-eight respondents interviewed believed that current interfaces could not support real-time interactive secure transmissions of data between these two systems.

AUTODIN can support classified transmissions, but it will not provide a real-time interface between computer systems with different security levels (3,33,54). AUTODIN lacks the design mechanisms and the trusted software required to become a trusted system (6,41).

Secure transmissions can be accomplished using AUTOSEVCOM, DDN, and encryption/decryption devices. While technically it is

not a problem to transmit data from a computer with a lower classification to one with a higher classification, transmission of data from higher classified computers to lower classified computers is a problem. And since computers are normally set up to both send and receive data, the Joint Chiefs of Staff have expressly prohibited such an operation (39:3-2-1). A security filter is needed to examine data, element by element, to determine if the DSACS user can access the data in CAS. The filter will also have to examine data before it is transmitted to the DSACS user to insure that only that data which was requested and authorized for release is transmitted (33).

DISNET can support the real-time interactive transmission of data up to only the Secret level. However, DISNET is confined to a system high mode of operation (32).

The consensus of opinion among the respondents highlights the fact that current interfaces are too vulnerable to be trusted under the circumstances to which they will be applied. Both inadvertant and forced disclosure can still occur in WWMCCS (59). The system high mode prevails among the current systems.

Three respondents answered question 2 affirmatively. One respondent categorized the Secure Communications Processor (SCOMP) as a current system designed to provide for the proper secure interface (See Appendix D) (57). Another respondent felt that the Restricted Access Processor (RAP) was a current

system which could solve the problem (See Appendix I) (55). The third respondent listed the Advanced Command and Control Architectural Testbed (ACCAT) Guard, the FORSCOM Security Monitor, the Large Scale Integration (LSI) and Korean Air Intelligence System (KAIS) Guards, and the RAP as current interface methods that should be investigated (See Appendices D through I) (37).

The intent of the question was to find out what current and operational interfaces exist that could solve the problem. To date, although a few of these interfaces are coming closer to operational status, none are in service.

Interview Questions 3 and 4. The responses to these two questions were addressed together because most of the respondents answered these questions together.

Thirteen respondents believed that both DSACS and CAS should not remain at their present levels of classification (1,3,5,13,29,32,33,35,37,38,54,58,67). Until a multilevel secure filter is implemented, either one or the other system would have to change security levels so that both systems could function on a system high mode and transmit data on a real-time basis (5,35,38,47,50,54,64,67). The National Security Agency (NSA) is charged with approving any systems/hardware interfacing with WWMCCS. Until NSA approves a multilevel secure interface between DSACS and CAS, an unclassified DSACS will not be allowed to be directly linked

to the WIN (3,13,54). However, according to JCS and Air Force policy, CAS must remain in WWMCCS (9,67). The SMCA policy concerning the classification of DSACS is equally inflexible (9). This dilemma has some of the respondents concerned about a number of issues.

Respondents were concerned that DSACS could easily compile enough unclassified data elements, and form some information which might need more protection than an unclassified system can provide (9,32,33). Another problem is that data or information that the Air Force would protect under a level of classification may not necessarily be classified by the Army at the same level (9,48). The resolution of this issue will require a joint reexamination of Air Force and Army philosophies and policies on security matters (48,55).

A number of possible real-time solutions were offered as a means to allow CAS and DSACS to securely exchange data without changing the levels of security, and without the implementation of any security guard. One method would involve CAS acquiring a small computer which could be set up parallel to the CAS at HQ AFLC. All unclassified data that would be required by DSACS could be loaded on the smaller computer which could then be connected directly to DSACS. This system would not be connected to the WIN and would be real-time interactive with DSACS (47,53). Another idea would

be to interface DSACS to each of the major commands at the point where they make their transmissions to the WIN. At this interface point the data would not yet have entered the WIN and would not be subject to the additional restrictions that an unclassified connection to the WIN would involve (23). It may be possible to set up a two way unclassified exchange of data at that level without involving CAS directly in the loop (28).

Five respondents felt that the development of security guards like SCOMP and other trusted computer hardware and software could eventually allow CAS and DSACS to maintain their desired levels of classification (6,9,14,29,57). However, four respondents commented that even with the guard technologies in place, the degree of interrogation of either system by another will be severely limited. The strict format that the inquiries will have to conform to in order to conform to the security policy being enforced will prevent open interrogation (37,50,51,64).

Interview Question 5. The responses to this question were almost evenly distributed between positive and negative replies. Fourteen respondents stated that current interfaces could not be used to interface DSACS and CAS. Twelve respondents felt that current and/or developing interfaces could be applied to interface the two systems. Two respondents were unable to provide an answer to this

question.

All the respondents who said no to this question cited various deficiencies in current technology which, at present, would prevent a suitable interface between CAS and DSACS (1,3,6,13,14,29,31,35,37,51,53,54,58,64). A number of these respondents agreed that the physical interfacing of dissimilar systems (IBM and Honeywell) was not the problem. Current technology's inability to provide an NSA approved multilevel secure environment was cited as the major problem (1,6,13,14,29,31,35). Additional protocols need to be written to control user access to data with CAS (14,31). Not only must additional protocols be developed, but also whatever protocols are written must be adopted by both CAS and DSACS together (13).

Current efforts to develop multilevel secure environments have been unable to offer a solution which will allow CAS and DSACS to operate as they want and still be in compliance with WWMCCS security policy (3,51,53,54,58,64). Operating in a system high classified mode is against SMCA policy (43). Connecting CAS to an unclassified data base is prohibited by the WWMCCS ADP System Security Manual (39:3-2-1). And finally, removing CAS from WWMCCS in order to link it with DSACS is against Air Force policy (3,9,54). There is some hope caused by recent efforts to ease and revise WWMCCS policy with regard to less than Top Secret

communication links with WWMCCS. This effort, however, depends on the progress of the SCOMP and the FORSCOM Security Monitor (51).

The twelve respondents who expressed more positive opinions on the ability of current interface methods to provide a solution were more willing to endure the somewhat slow progress of the security guards. They were also more willing to compromise on some of the original interface requirements cited in Appendix A in order to preserve the levels of classification for both CAS and DSACS. One respondent felt that public domain software would be able to provide an interface, but only on a system high mode requiring a DSACS upgrade (38).

Four respondents offered the concept of a batch interface between the two systems involving the exchange of magnetic tapes via AUTODIN (5,9,28,67). This method is neither supportive of real-time exchanges of data, nor is it interactive, but it is well within current technology and appears to violate no policy.

Two respondents maintained some hope that current protocols could provide an interface between CAS and DSACS using the H716 front-end-processor co-located with CAS to manually downgrade data to an unclassified level for transmission to DSACS. One respondent felt that current protocols known as the Electronic Industrial Association

Recommended Standard Number 232 (RS232) and the Institute of Electrical and Electronic Engineers Recommended Standard Number 488 (IEEE 488) could be used to interface once the data had been downgraded (32). Another respondent felt that DDN will soon be used as the connecting network. The December 1983 version of the Consultive Committee on International Telephone and Telegraph Public Data Network Recommended Standard for Packet Switching, Number 25 (X.25) protocol could be used to connect CAS and DSACS to DDN (47). The X.25 is a network access and transport protocol. Also required for this interface would be a General Telephone and Electric Corp. Network Standard Virtual Terminal Protocol (Telnet), File Transfer Protocol (FTP), and Simple Mail Transfer Protocol (SMTP). Telnet is a virtual terminal protocol which converts traffic from different terminals so that a common format can be used on the network. FTP allows file transfer between dissimilar systems. SMTP supports the transfer of mail over DDN (47).

Five respondents felt that a number of guard systems would soon be able to provide a multilevel interface between CAS and DSACS (48,50,55,57,59). The FORSCOM Guard still requires an Air Force and Army evaluation, but if approved by NSA, the FORSCOM monitor would require relatively minor modifications before it could be implemented (57). The SCOMP hardware package could be used if an application program

could be written and certified by NSA (48). RAP would also require NSA certification and an Air Force and Army evaluation (55,59). The ACCAT Guard could be used if the requirement for real-time exchanges of data was made more flexible. However, NSA certification would still be required (50).

Interview Question 6. Many developments are in progress or being planned in the area of multilevel secure data processing. The Air Force Computer Aquisition Command (AFCAC) at Hanscom AFB MA, the DOD Computer Security Center (CSC) at Fort Meade MD, the Defense Intelligence Agency (DIA) at the Pentagon and the Air Force Data Systems Design Center at Gunter AFS AL are working on solving the multilevel security problem in the management of classified automatic data processing (1,6,32,38,47,57,67). The NSA and functional personnel within the WWMCCS and DDN communities are working to develop a multilevel secure capability within communication networks (1,6,38,47,57). Two developments which are beginning to come out of these efforts are the Internet Private Line Interface (IPLI) and the Blacker Device (6). (See Appendix J).

A number of government agencies outside of the Department of Defense also have an interest in this area. The Department of Transportation, the Department of Energy, the Federal Government, and the National Aeronautics and

Space Administration (NASA) are all working on computer security issues (50).

Commercial vendors are showing an increasing interest in computer security. Martin Marietta, TRW, and Systems Development Corp have research and development projects ongoing with context dependent security guards (50). During the last eight years much progress has been made in the area of multilevel secure data transmission (55). No less than twelve trusted computer system projects have been intiated and/or completed during this time (63:111-113). These trusted systems were built by the University of Texas, Christian Rovsing, the Naval Post Graduate School, Honeywell, Digital Equipment Corp, Logicon, I.P. Sharp Inc., Ford Aerospace and Communications Corp., Computer Sciences Corp., Sytek Inc., Systems Development Corp., Gemini Corp., and Royal Signals and Radar Establishment (England) (63:111-113).

A number of specific multilevel security projects are beginning or continuing studies and tests to further their development and aid in the evaluation process. The FORSCOM Guard Project is part of FORSCOM's study to deal with dissimilar levels of security in data transmission (6,48,51,64). The Honeywell SCOMP hardware will begin operational testing during the fall of 1985 (5,58). The RAP Guard is in testing at this time (55,59).

Many of the respondents found it difficult to address the estimated time before the secure systems could be implemented. Certainly, NSA certification and approval is beyond the control of those companies building the systems. However, estimates were made for a number of systems.

The Defense Data Network already has an interface with IBM mainframes and with WWMCCS, but it still lacks some software program development. Once the software programs are ready it will take less than a year to implement (13). In addition, DDN should be able to implement its Blacker Device in 3-4 years (47).

The RAP Guard has been implemented and is presently functioning, but has not yet been applied to the DSACS/CAS interface. Computer Sciences Corp. is in the process of manually performing formal mathematical proofs to verify that the RAP's security design corresponds to its security model and enforces its security features. They are also trying to develop an automated method of verification which, if discovered soon, could speed the implementation of the RAP Guard in other applications. Automated verification may take three years to develop (55).

The Honeywell SCOMP provides the hardware necessary for multilevel secure processing; however, software must be developed and accredited for any new applications. It is estimated that 2 years would be a minimum time necessary to

develop software for the SCOMP (5).

Respondents in support of DDN, RAP, and SCOMP were able to make some general statements about the outlook for expanded capabilities of these systems. DDN, RAP, and SCOMP all have an excellent potential for expansion (47,51,55,59).

DDN will be the communications network which will eventually carry multilevel secure transmissions for all DOD ADP systems (18:1). "The DDN backbone will grow to be a highly survivable network of several hundred packet switches located throughout the world" (See Appendix J) (18:3). DDN can become a more powerful network once it incorporates a secure front-end processor like the RAP or SCOMP (13,57).

RAP could enhance its capabilities by developing more access codes which would allow, for example, access to CAS and DSACS from different levels of command within the DOD. This expansion could be done with the end-to-end encryption of data (See Appendix I) (55).

SCOMP has already begun to expand its potential in multilevel security systems. The SCOMP is basically a piece of secure hardware for which any number of software programs can be written according to the formal security policy which needs to be applied in any new application. The SCOMP is presently being implemented on the ACCAT Guard and the FORSCOM Security Monitor, but it also has additional potential.

In addition to its potential guard applications, the SCOMP system is being evaluated and considered as a base for a variety of applications that require its security features. Some of these applications are data base management, office automation, message processors, and general purpose systems (63:192).

Interview Question 7. Each respondent who offered an answer to this question will have his or her answer listed individually. This technique will be used to insure that each individual response will be as accurate as possible.

-It appears that the only solution is interim at best. That solution would be to batch interface CAS and DSACS using an H716 front-end processor as a "holding tank" to ensure that data received from the WWMCCS is really unclassified prior to transmittal via AUTODIN. If we can achieve this batch processing enough times during the day (4-6 times), it may be close enough to real time to suffice as an interim solution (3).

-The Air Force should use the M024 AUTODIN system with an "air gap" of unclassified extract from the classified CAS WWMCCS system (54).

-The Air Force should follow the Army's lead established with the FORSCOM Guard Project. The Air Force should investigate and keep track of Army WWMCCS Information System Project Management Office progress with the SCOMP applications (58).

-The Army should investigate the use of the available WWMCCS Intercomputer Network connections from FORSCOM to allow DSACS to access the CAS (33).

-The Air Force should define the functional security requirements first. Then it should start an air gap interface to fine tune their statement of requirements - back it up with some results and experience. Discuss the long term solution with software controls if needed. Decide whether real-time transmission is really needed (67).

-The Air Force should pursue a system high mode of

operation. Interface requirements must be addressed in the developmental stages by design engineers from both the Air Force and the Army. Good communication between each service is the key (32).

-The Air Force should separate the unclassified data from CAS and place it on a microprocessor and use DDN to exchange unclassified data between CAS and DSACS (47).

-The Air Force should embrace the WWMCCS Information System development to look for possible solutions (57).

-The Air Force should make an unclassified microcomputer data base from the CAS and set it up parallel to the WWMCCS and interface on an unclassified system high connection to DSACS. Reevaluate the need for real-time interaction. If real-time interaction is so important, then there must be a system high Top Secret connection between systems. The Army would have to upgrade their system to Top Secret (38).

-The Air Force should investigate all guard technologies. Either DSACS must upgrade to Top Secret or some form of guard technology must be used between the two systems (37).

-The Air Force should look into RAP Guard applications. Honeywell Inc., has the lead in this area now because of the SCOMP hardware (55).

-The Air Force should make an unclassified data base parallel to CAS. Update the unclassified CAS parallel computer manually every day. This procedure can be done now. The Air Force should do this because we do not trust computers to do all the security monitoring and protecting of data. Computers can be sabotaged. If a computer should make a mistake and transmit some classified data, a tremendous amount of unauthorized data can be released in a short time. Human errors would not normally result in such a large compromise (6).

-The Army should upgrade DSACS to Top Secret or the Air Force should find a way to process information on less than a Top Secret system high mode. In the meantime, SCOMP is hardware that has been certified

for multilevel security processing. FORSCOM software is in the process of being certified (5).

-The Air Force should become involved with other agencies which have needs for the protection of ADP information systems. The Department of Agriculture and General Motors have similar problems with interfacing computer systems which provide for security of their data. Use these inputs to help develop a strategic plan to determine how to deal with the problem of linking these two systems. The recommended approach is the one that will be long-sighted and one that will have a generic applicability towards similar problems with other agencies. Shy away from quick short-sighted systems which may only apply to CAS and DSACS for the present (14).

-The Air Force should try to establish a common structure for the protocols necessary to protect information. There seems to be an unnecessary proliferation of software being developed by the vendors. The X.25 protocols are a suitable standard which could be adopted by more vendors. I recommend more standardization and communication among those companies and government functions which are interested in computer security (41).

-The Air Force should send more questionnaires like this out to the vendors to help make them aware that there is a need and a requirement for multilevel security (35).

-The Air Force should keep all ammunition data classified. The Army should upgrade DSACS to Top Secret (53).

-The Army needs to tell the Air Force exactly what DSACS needs from CAS and how soon or often it really needs this information. This must be done while CAS is still in development. The Army should reappraise their needs and requirements because the timeliness and refinement of the information requested will drive the requirements. As the degree of detail of the data and the timing of data transmitted reaches upper limits, the WWMCCS Intercomputer Network becomes less of a potential solution because DSACS will have to become Top Secret (28).

-The Air Force should study the SCOMP hardware because it has been certified A1. The Air Force needs to communicate more with the DOD Computer Security Center to help define the security validation requirements before any software is developed. The Air Force should determine exactly what information is required to be shared by each system (48).

-The Air Force needs to reevaluate the requirements to interface CAS and DSACS. A detailed analysis of the two applications must be done to insure a well defined requirements definition (51).

-The Air Force has three alternatives. The simplest alternative is to require that DSACS become Top Secret which requires no new technology. The second solution would be to make CAS a trusted system which requires state-of-the-art technology and is still 3-4 years away. The third solution is to have a guard device with a man in the loop. It would incur certain personnel expenses to maintain a man in the loop, but it would not require CAS to become a trusted system (50).

-The Air Force must recognize the problem and realize that it needs a better solution than an air gap interface. The problem is the security of the data and not a lack of interface technology. Investigate SCOMP and Blacker technology (1).

-The Air Force and the Army should operate on the same level of security (13).

-The DOD must decide on a specific protocol between the local systems and the local node of the DDN network (29).

-The Air Force and the Army must format their data in a very rigid form so that the parameters of the data can easily describe the criteria which will pass only the correct data to each system. Only then will a security filter be effective and trusted (64).

Summary of Major Findings

A summary of the major findings which provides answers to the investigative questions is presented below.

1. What requirements will an interface method have to meet to be acceptable to both DSACS and CAS?

- The major requirements for an interface will have to focus on the security issues raised by linking DSACS and CAS together without changing their security classifications (6,37,55,59).

- The Army and Air Force need to implement a trusted computer system as a security guard to satisfy the requirements of a multilevel secure mode of operation (13,37).

- The DOD Trusted Computer System Evaluation Criteria, CSC-STD-001-83, contains six major requirements that a trusted computer system must have in order to be certified as "secure".

- There must be a well defined security policy enforced by the system.

- Every data element in the trusted system must be marked with a label that identifies its classification.

- Each user must be identified and their access to the system restricted to only authorized data.

- All transactions must be traceable with an audit function.

- The system must have trusted mechanisms which can be independently evaluated to assure that all the above requirements are met.

- The trusted mechanisms must be continuously protected to avoid unauthorized modification (19).

2. How well can current technology support these requirements?

- No current interface method allows for real-time interactive secure transmission of data between dissimilar systems (64).

- Current interface methods exist which would not require CAS and DSACS to change their security levels. However, these methods can not support both free interrogation capabilities and real-time exchanges of information (5,9,28).

- Any security guard will force inquiries into classified systems to be strictly formatted. Complete freedom to interrogate systems will not be possible (37,50,51,64).

3. What are the various interface methods currently in use?

- AUTODIN, AUTOSEVCOM, DISNET, DDN, WIN are current communications system which are capable of transmitting classified data (3,6,13,28,33,38,41,47).

4. What is the best method of interface?

- A few developing security guards can filter classified data from classified computer systems before transmitting the data to computer systems operated at lower levels of classification.

- The ACCAT Guard (37,8)
- The FORSCOM Security Monitor (58,8)
- The Large Scale Integration Guard (37,8)
- The Korean Air Intelligence System (37,8)
- The Restricted Access Processor (55,59)
- Secure Communications Processor (5,63)

- Many developments are in progress or being planned in the area of multilevel secure data processing (1,6,32,38,47,57,67).

- The Air Force, Navy, and Army have interests in multilevel secure data processing (1,6,32,37,38,47,57,67).

- Commercial vendors are becoming more interested in computer security (50).

- The Department of Transportation, the Department of Energy, and NASA are working on computer security issues (50).

Selection of Alternatives

The respondents identified nine computer systems or interface methods which were identified as having attributes which could be applied to help solve the interface problem between DSACS and CAS. These computer systems were identified as follows:

Appendix D:	Secure Communications Processor (5,57)
Appendix E:	The ACCAT Guard (37)
Appendix F:	The FORSCOM Security Monitor (58)
Appendix G:	The Large Scale Integration Guard (37)
Appendix H:	The Korean Air Intelligence System (37)
Appendix I:	The Restricted Access Processor (55,59)
Appendix J:	The Defense Data Network (47)
Appendix K:	Unclassified Parallel Interface (38,47)
Chapter II:	Proposed CAS-DSACS Interface (3) (To be known as The Air Gap Interface)

These nine computer systems were screened as candidate alternatives for final evaluation using the selection criteria and the rationale described in Appendix C. SCOMP, RAP, Unclassified Parallel Interface, and Air Gap Interface were selected for final evaluation.

SCOMP was selected for further evaluation because it had been identified as a versatile piece of hardware which had been certified by the DOD Computer Security Center as having satisfied A1 trusted computer system evaluation criteria (57,64). According to the DOD Computer Security Center an A1 certification is required when an unclassified computer system is linked to a Top Secret computer system (23:14).

RAP was selected for further evaluation because it was a hardware computer system specifically designed to interface classified computer systems with unclassified computer systems. RAP specifications are designed to satisfy the A1 trusted system criteria (52). RAP is also a real-time interface which experiences no service degradation throughout the mediation process (52,55,59). A1 certification is expected (63:114-115).

The Unclassified Parallel Interface was selected for further evaluation because it was a readily available method of allowing unclassified information to be transmitted from CAS to DSACS. It does not require DSACS to upgrade its system to Top Secret and does not require CAS to downgrade its system. Information resident within this unclassified computer can be transmitted in real time to DSACS. DSACS could also send unclassified information to the CAS parallel system (6,47).

The Air Gap Interface was selected for further evaluation because it also is a readily available method of interfacing DSACS and CAS without forcing either system to change their security classification. The Air Gap Interface was also selected as a possible alternative by DSACS and CAS functional personnel (42).

The ACCAT Guard, LSI Guard, KAIS Guard, FORSCOM Security Monitor, and DDN were not selected for further evaluation.

These systems were not selected because of some fundamental reasons.

The ACCAT Guard and the FORSCOM Guard are systems which are implementing the SCOMP system as the trusted hardware of their systems (63:192,7). The performance of the SCOMP in these systems will largely determine the trustworthiness of the guards. Therefore, only SCOMP was evaluated as the essential piece of hardware.

The KAIS was recommended once, for use only in combination with the LSI Guard (37). Since the LSI Guard is not expected to attain higher than a B3 evaluation by the Computer Security Center (CSC), the combination of the LSI and the KAIS was also not chosen for further evaluation (63:114-115).

DDN was not chosen for further evaluation simply because it is not a security guard system. DDN is a communications network which requires interfaces at every node (18:10). DDN would enable a security guard to have access to any DDN user and would allow multilevel secure message traffic flow on the network. The problem with DDN is that without a security guard, a Secret system can not use the network to send information to a receiver which has a lower security classification (13). DDN and guard technologies can only complement each other.

Analysis of Alternatives

A decision matrix was developed in Chapter III to show the rank order of the alternatives with respect to the degree to which they satisfied a number of selection criteria. Four alternative were ranked on an ordinal scale to show their relationship to each other when judged individually against each of six selection criteria (See Figure 4). Selection criteria chosen by the researcher were:

1. Time to implement the alternative interface method.

2. Interoperability of the CAS and DSACS systems allowed by the alternative method.

3. Security. The ability of the method to protect classified information from being accessed by unauthorized users of the two systems.

4. Expandability. The potential for the alternative method to be incorporated into a larger network of computer systems at a later date.

5. Permanence. The possibility that the alternative represents a permanent solution.

6. Real Time. The relative speed of processing and transmitting information between CAS and DSACS.

The alternatives to be ranked are the RAP Guard, the Secure Communications Processor (SCOMP), the Unclassified Parallel Interface, and the Air Gap Interface. Each alternative will be listed under each individual criteria in the order of its rank, the number one ranked alternative being listed first. As each alternative is ranked, it will

also be justified.

Real Time. (1) RAP - The RAP Guard is the only guard which can support real-time exchanges of data. There is no service degradation caused by the mediation process of the security mechanisms (52,55,59).

(2) SCOMP - The SCOMP suffers between 5 to 15 percent service degradation caused by the mediation process of the security mechanisms (63:189).

(3) Unclassified Parallel Interface - This interface can operate in real time; sending unclassified data to DSACS, and receiving unclassified data from DSACS (6,47). However, the unclassified computer must receive updated information from CAS in order stay current. This updating will take time and would involve a review process (6).

(4) Air Gap Interface - This interface requires that CAS unload data to a front-end-processor for manual review. Once the data have been screened, it must be loaded on a magnetic tape and sent to DSACS via AUTODIN (3,32,54,67). This interface is extremely slow and cumbersome.

Time to Implement. (1) Air Gap Interface - The practice of batch processing magnetic tapes is a well known procedure which requires no new developments (3,54).

(2) Unclassified Parallel Interface - A new computer must be bought, installed and set up, but there would be no difficult security evaluation process or new technology

introduced (6).

(3) SCOMP - SCOMP has already been evaluated and certified an A1 system. A SCOMP is a modified Honeywell DPS 6 computer, the basic model of which is used daily in WWMCCS nodes (5,36).

(4) RAP - The RAP is being evaluated at this time and has not yet been officially certified as an A1 system. It is fully expected to receive the A1 cetification soon (55,59).

Security. (1) RAP - The Rap Guard follows DOD Central Security Center evaluation criteria for trusted systems and has been specifically designed from inception to connect unclassified systems to classified systems (8,52,55).

(2) SCOMP - The SCOMP also follows the DOD CSC criteria and has been certified as an A1 system, but so far, the environments in which it has been tested involve linking only two classified systems (Secret and Top Secret) (8:6,37).

(3) Air Gap Interface - There is no formal security policy agreed upon by both the Army and Air Force embedded in the security review that must be done. There is a risk that an aggregation of unclassified data at DSACS could become classified by Air Force standards (48).

(4) Unclassified Parallel Interface - Normally there is no security risk involved with a system high unclassified computer, but the security of the mechanism needed to get the unclassified data from CAS to this computer remains in

question. Also, when the unclassified computer is operating on-line with DSACS the amount of data (and possible compromises) that could be transmitted would be enormous (6).

Expandability. (1) SCOMP - The Honeywell DPS 6 is a well known piece of hardware which already has extensive links set up within the WIN. The SCOMP was designed to use a modified DPS 6 in the WWMCCS environment (5).

(2) RAP - The RAP uses a different piece of hardware (Intel 286, VAX 11/730) than what DSACS and CAS are using (IBM, Honeywell). The RAP hardware is reported to have very adaptable features (52).

(3) Unclassified Parallel Interface - This interface is not likely to be expanded because of the problem of updating the unclassified portion of the interface. This interface also seems to circumvent the security issue.

(4) Air Gap Interface - This solution was only offered as an interim solution by DSACS and CAS. It is too slow and cumbersome to be worthy of expansion (42).

Permanence. (1) SCOMP - Honeywell Inc., continues to support the WIN and the area of multilevel security very well. As long as SCOMP continues to develop, it will have a long future in the WIN.

(2) RAP - DSACS and CAS are still very much interested in achieving real-time interfacing. RAP is the only system which is real time and will be multilevel secure (55,52,59).

(3) Unclassified Parallel Interface - The need for multilevel secure computer systems is increasing every day (63:108). This interface circumvents the problem.

(4) Air Gap Interface - The interface requirements cited in Chapter I clearly state a need for real-time interfacing capabilities. A system which can never achieve this goal should not be considered a permanent solution.

Interoperability. (1) RAP - If RAP is successful in bridging the gap between Secret and unclassified users, it will increase the DOD's ability to communicate with a much wider communications community than any other system.

(2) SCOMP - Although SCOMP is already certified an A1 system, it has not yet attempted to bridge as wide a security gap as the RAP. Until SCOMP also attempts to link unclassified users with classified users, it will not be able to communicate with nearly as many computer systems.

(3) Air Gap Interface - The Air Gap interface must rely on a slow review process and magnetic tape batch interfacing to interact with any other computer system. A separate review process would have to be accomplished and a separate magnetic tape would have to be made in order to communicate with different user security classification levels.

(4) Unclassified Parallel Interface - This unclassified interface will be unable to receive any data from a computer system which is classified. Any classified system would have

to use a security guard to sanitize the data before transmitting to this computer.

The alternatives, once ranked against each of the six criteria, were placed in a matrix. Each criterion was placed in a row of the matrix and each alternative was placed in a column of the matrix. The ordinal ranks were then summed for each alternative.

	Alternative			
	A1	A2	A3	A4
Time	1	3	4	2
Interoperability	3	2	1	4
Security	3	2	1	4
Expandability	4	1	2	3
Permanence	4	1	2	3
Real Time	4	2	1	3
Rj	19	11	11	19

Rj - The sum of the rank for each alternative.

Alternative A1 - Air Gap Interface

Alternative A2 - Secure Communications Processor

Alternative A3 - The Restricted Access Processor

Alternative A4 - Unclassified Parallel Interface

Determination of the Kendall Coefficient of Concordance: (W)

The method for determining the Kendall Coefficient of Concordance was explained in Chapter III. The calculations based on the the ranking of the alternatives are as follows:

Calculations.

1. Let N = 4, the number of alternatives to be ranked and let k = 6, the number of selection criteria.

2. For each alternative, determine Rj, the sum of the ranks assigned by the 6 selection criteria. Rj = 60.

3. Find the mean of the Rj ($\bar{R}j$). Express each Rj as a deviation from that mean, square the deviation and sum the deviations to get s.

$$\bar{R}j = Rj/N = 60/4 = 15 \quad (1)$$

$$s = \Sigma(Rj - \bar{R}j)^2 \quad (2)$$

$$s = (19-15)^2 + (11-15)^2 + (11-15)^2 + (19-15)^2$$

$$s = 64$$

4. There were no ties in the rankings, therefore, equation 5 will be used:

$$W = \frac{s}{.083k^2 (N^3 - N)} \quad (5)$$

$$W = \frac{64}{(.083)(36)(60)} = .35$$

$$W = .35 \quad s = 64$$

Test of Significance

In order to test the W for significance, test the null hypothesis that the 6 sets of rankings are independent.

Table I was used to check for significance. The observed s = 64, was less than the critical value (s = 75.7) for k = 6 and N = 4. The null hypothesis can not be rejected, therefore, W is not significant.

Interpretation of the W Statistic. The fact that the W was not significant indicates that a clear one best choice could not be made based on the six selection criteria. The sums of the ranks of the alternatives when compared to the selection criteria resulted in a pair of ties. The pair of ties had the effect of lowering the value of s. Note equation 2. The difference between the Rj and the mean of all Rj was small and when the differences were squared the resulting s was small.

The resultant value of s implies that the six criteria were independent. The alternatives were ranked high against some criteria, but low against others. If the criteria were dependent, an alternative that satisfied one criteria very well would also satisfy other criteria. Consistent rankings would be expected for alternatives which were ranked by criteria which displayed more dependence. This was not the case. Each alternative had a wide range of rankings against the criteria.

The difference in the values of each paired sum (11 versus 19), however, indicates that the RAP and the SCOMP are alternatives which satisfy the six criteria better than the

Air Gap and Unclassified Parallel Interface. The "best interface" appears to be one which can act as a secure filter between DSACS and CAS. This methodology was unable to determine which of the two multilevel secure guards would be best.

Summary

This chapter presented the findings and an analysis of the results of the thesis effort. The chapter began by presenting the results of the telephone interviews. The second section summarized the major findings of the thesis. The third section justified the selection of four alternatives which represented possible solutions to the CAS/DSACS interface problem. The fourth section presented an analysis of the four alternatives using the methodology described in Chapter III. The Kendall Coefficient of Concordance was performed on the data collected and was found not to be statistically significant. Finally, the resulting W statistic was interpreted to indicate the six selection criteria were independent and not capable of selecting the "one best" alternative. However, the criteria seemed to indicate that two alternatives were equally qualified as the "best" alternative. The next chapter will contain conclusions and recommendations for further study.

V. Conclusions and Recommendations

Introduction

This chapter will present the final conclusions and recommendations that resulted from the thesis effort. The first subheading will present an overview of the esearch. The second subheading will provide conclusions and recommendations based on the results and findings of the thesis.

Overview

Chapter I introduced the general issue of the thesis, offered a brief background on the issues and provided the justification and the scope of the research effort. The lack of an acceptable interface between the Air Force's Top Secret Combat Ammunition System (CAS) and the Single Manager for Conventional Ammunition's (SMCA) Defense Standard Ammunition Computer System (DSACS) was identified as the specific problem. The scope of the research was limited to single manager assigned conventional ammunition data of interest to the SMCA and the Air Force. Four investigative questions were identified to provide a framework for the research and to provide the information necessary to develop a proposal for an alternate method of interface.

1. What requirements will an interface method have to meet to be acceptable to both DSACS and CAS?

2. How well can current technology support these requirements?

3. What are the various interface methods currently in use?

4. What is the best method of interface?

Chapter II provided a literature review which offered a historical perspective of conventional ammunition management over the past 45 years and documented a trend towards centralized ammunition management. The literature review served to highlight the need for the DOD to develop a centralized ammunition management concept to provide for a long-range planning capability and to avoid costly plant start-ups and duplications of effort among the services. DSACS and CAS were designed, in part, to provide more visibility for wholesale and retail conventional ammunition as part of the military's trend towards improved centralized management of ammunition. The lack of an acceptable interface between these ammunition computer systems is serving to limit their potential capabilities.

Chapter III offered a methodology which was designed to provide answers to the investigative questions. A structured telephone interview was designed to be given to a sample population of twenty-eight computer experts. The structured telephone interview contained seven questions. (See Appendix A). The interview questions were designed to answer the four

investigative questions which were first mentioned in Chapter I.

The first investigative question was designed to determine what requirements were necessary to satisfy the needs of CAS and DSACS. Therefore, it was restated as the first interview question. The second and third investigative questions were designed to determine if current technology could support these interface requirements and whether or not such technology existed today. Interview questions two, three, four, five and six were designed to answer the second and third investigative questions by making an assessment of the current state of technology. The seventh interview question was designed to encourage comments on what areas the Air Force should concentrate on to solve the interface problem. Finally, the analysis of the findings was designed to answer the fourth investigative question: What is the best method of interface?

Chapter IV presented the findings and provided an analysis of the results of the thesis effort. Four alternatives which best conformed to the original interface requirements cited in Chapter I were selected for further evaluation. The alternatives were ranked individually against each of six criteria according to the methodology explained in Chapter III. The next subheading will provide the conclusions and recommendations of the thesis.

Conclusions and Recommendations

An analysis of the major findings of the thesis and the four chosen alternative interface methods has lead to the formation of a number of conclusions and recommendations. The conclusions and recommendations based on the experts' answers to the investigative questions are presented below.

Investigative Question 1. What requirements will an interface method have to meet to be acceptable to both DSACS and CAS?

Conclusions. The major requirements for an interface must focus on the security issues raised by linking DSACS and CAS together without changing their security classifications. Seventeen of twenty-eight respondents felt that the major requirements necessary to interface CAS and DSACS would not revolve around the issue of real-time interactivity or free interrogation capability, but instead, would have to focus on the security issue of linking the unclassified DSACS to the Top Secret CAS.

A computer system is required to create an on-line interface which can be trusted to filter Top Secret classified data from unclassified data in CAS before transmitting the unclassified data to DSACS. Nine respondents felt that in order to bridge the gap between two computer systems of different security levels, a trusted security filter would be necessary to insure that

unclassified data transmitted from CAS to DSACS would be trusted not to contain any classified data.

The trusted computer system must at least satisfy the six fundamental security requirements cited in the Department of Defense Trusted Computer System Evaluation Criteria, CSC-STD-001-83. At least seven respondents cited this publication, informally referred to as the "Orange Book", as one of the absolutely essential references that would contain the security requirements necessary to interface CAS and DSACS. The Orange Book addresses the development of a statement of requirements for computer security by describing six requirements necessary to define a computer system as "secure". The six requirements deal with the security policy, the accountability and assurance measures necessary for a computer system to become trusted. The requirements basically cover the need for a trusted computer to control access to information and the need to prove that such control is actually accomplished. The six requirements and associated evaluation criteria are presented in Chapter IV under the results subheading for interview question 1.

The trusted computer system must satisfy the trusted computer system evaluation criteria minimum requirements for a class A1 verified design. According to the Computer Security Center publication, Computer Security Requirements - Guidance for Applying Department of Defense Trusted Computer

System Evaluation Criteria in Specific Environments, CSC-STD-003-85, linking an unclassified data base to a Top Secret data base requires the verified protection afforded only by a criteria class A1 certification.

Recommendations. The Air Force and Army should reevaluate the interface requirements for DSACS and CAS. The major interface requirements that should be reconsidered are the need for a real-time interface and the need for a free interrogation capability.

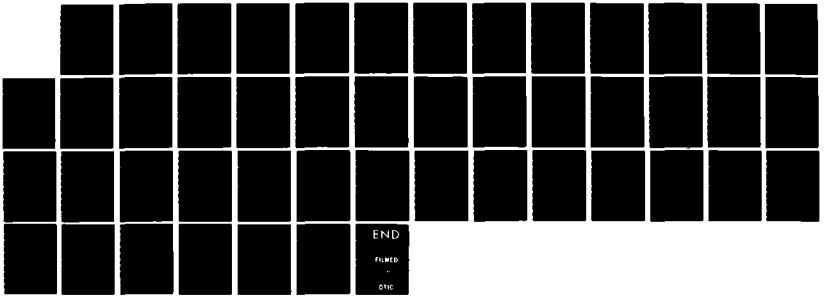
As part of the reevaluation, the Air Force and Army should define their concept of real-time interaction and free interrogation. This definition of terms should be accomplished before the services can specifically define the interface requirements needed to support the concepts.

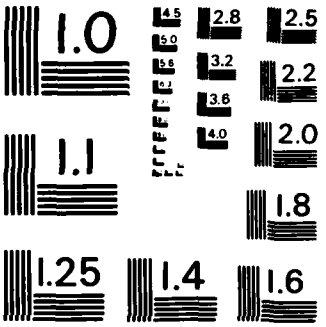
The CAS and DSACS design engineers should establish an open dialogue on the definition of terms and system requirements while each system is still in the development stage.

If the current interface requirements are to be met, CAS and DSACS design engineers should begin to consider the application of multilevel secure interfaces to their particular environment.

AD-A161 332 INTERFACING THE DEFENSE STANDARD AMMUNITION COMPUTER SYSTEM AND THE AIR F..(U) AIR FORCE INST OF TECH WRIGHT-PATTERSON AFB OH SCHOOL OF SYST.. A C JONES 2/2

UNCLASSIFIED SEP 85 AFIT/GLM/LSM/85S-39 F/G 15/5 NL





MICROCOPY RESOLUTION TEST CHART
NATIONAL BUREAU OF STANDARDS - 1963 - A

Investigative Question 2. How well can current technology support these requirements?

Conclusions. Twenty-two of the twenty-eight respondents believed that no current interface method allowed for real-time interactive secure transmission of data between dissimilar systems. AUTODIN, AUTOSEVCOM and the WIN can support interactive and secure transmissions of data, but can not link data bases operating at different security levels. DDN and DISNET provide a communication network capable of carrying packets of data which may have different levels of security. However, the sender and receiver of data must operate in a system high mode. A more detailed description of DDN can be found in Appendix J.

A consensus of opinions among respondents highlighted the idea that current interfaces are too vulnerable to be trusted under the circumstances to which they would be applied. In fact, the Joint Chiefs of Staff support this idea and have expressly prohibited classified data bases from having on line interfaces with unclassified data bases.

Eight respondents believed that until a multilevel secure filter is implemented, either CAS or DSACS will have to change security levels so that both systems could function on a system high mode and transmit data on a real-time basis. Prior to implementation any application of a trusted computer system will have to be certified and approved by the DOD

Security Center.

Four respondents felt that any security guard will force inquiries into the classified systems to be strictly formatted. Complete freedom to interrogate systems will not be possible.

Recommendations. The CAS and DSACS designers should take into consideration the inability of state-of-the-art technology to provide a free interrogation capability in a multilevel secure environment when reevaluating the interface requirements. They should initiate research in multilevel secure data communications and develop work around solutions for the near future.

The Air Force and Army must seek out commercial vendors and other agencies which are involved with developing multilevel secure systems and establish an open dialogue between all concerned parties.

Investigative Question 3. What are the various interface methods currently in use?

Conclusions. AUTODIN, AUTOSEVCOM, DISNET, DDN and the WIN are current communications systems which are used within the Department of Defense. The interface method proposed for DSACS and CAS in January of 1985 involved the use of current AUTODIN capabilities as well as off-line batch interfacing. The AUTODIN off-line interface does not support real-time exchanges of data and is not very interactive.

This interface was described at the end of Chapter II. AUTOSEVCOM, DISNET, DDN and the WIN have not been implemented as connections between CAS and DSACS. As of 1982, the Department of Defense has been required to implement DDN as a common-user data communications network for all its ADP sytems. A more detailed description of DDN and its evolutionary strategy can be found in Appendix J. Although the WIN does not have a connection between CAS and DSACS, the Joint Chiefs of Staff policy has indicated that CAS will remain within its network.

Current protocols which allow different computer systems to interface are the RS 232, the IEEE 488, and the December 1983 version of the X.25. These protocols can, for example, enable an IBM mainframe to interface with a Honeywell mainframe, but have no ability to function as the interface between two computers operating at different levels of security. According to one respondent, there is an unnecessary proliferation of protocols being developed by vendors.

Recommendations. The Air Force and the Army should establish the X.25 as a standard for protocols necessary to protect information.

All interface designs should take into consideration that the WIN and DDN are here to stay and that a permanent interface will involve both these systems in some way.

Investigative Question 4. What is the best method of interface?

Conclusions. The analysis of alternatives in Chapter IV was unable to determine which alternative interface method was clearly the best by using the Kendall Coefficient of Concordance. No alternative was ranked consistently high or low enough against the six criteria to result in a large enough sum of squared difference of rank to indicate a significant W statistic. Honeywell's Secure Communications Processor (SCOMP) and Computer Sciences Corporation's Restricted Access Processor (RAP) appear to equally satisfy the six selection criteria used to select the best interface method for DSACS and CAS. These two methods each received a rank sum of 11. A more detailed description of the SCOMP can be found in Appendix D. The RAP is described in Appendix I. The Unclassified Parallel Interface and the Air Gap Interface did not satisfy the six selection criteria nearly as well as either of the above trusted computer security guard systems. These two methods each received a rank sum of 19. A more detailed description of the Air Gap interface (otherwise known as the Proposed CAS/DSACS Interface) can be found at the end of Chapter II. The Unclassified Parallel Interface is described in Appendix K.

Recommendations. The Air Force and Army should study both the RAP Guard and the SCOMP very carefully as two candidates for implementation as a multilevel secure interface between CAS and DSACS.

Appendix A: Sample Letter and Questionnaire

Capt Alan C. Jones
AFIT/LSG
Wright-Patterson AFB OH

Dear

I am a graduate student at the Air Force Institute of Technology, School of Systems and Logistics. I am doing a Thesis which involves searching for a better method of interface between two military ammunition computer systems: The Defense Standard Ammunition Computer System and the Combat Ammunition System.

The method of research requires expert opinion in response to questions which will be asked during our telephone interview. The objective of the interview is to gather information which may eventually lead to a better interface between these two systems. I will evaluate the results of the research and will forward recommendations to Ogden Air Logistics Center, Directorate of Materiel Management, Airmunitions Requirements and Distribution Branch and Headquarters, Army Armament Material Readiness Command.

I have enclosed an attachment which briefly addresses the general issue and specific problem of the research, the functional requirements for an interface, and the interview questions. Thank you for your time and assistance.

Alan C. Jones, Captain, USAF
Student, Air Force Institute of Technology,
School of Systems and Logistics

2 Encl

General Issue

The Army is the Single Manager for Conventional Ammunition (SMCA). A major objective of the SMCA is to develop a standard DOD-wide automated data base to improve defense wholesale munitions management. The Defense Standard Ammuniton Computer System (DSACS) is being designed to interface with existing service unique ammuniton data systems.

Specific Problem

The Air Force is developing the Combat Ammunition System (CAS), a TOP SECRET data system which will reside within the World Wide Military Command and Control System (WWMCCS). The DSACS data base will be unclassified and will not be able to directly access the data it requires from CAS with an on-line interface because of the security classification of the CAS data base. A method to interface the two systems needs to be proposed and evaluated.

Interface Requirements

1. The interface must not require DSACS to classify their system.

2. DSACS and CAS must be able to freely interrogate each other for any combination of data. Standard forms of interrogation alone will not fulfill this requirement.

3. The interface must support real time exchanges of information.

4. The interface must not force CAS to be removed from WWMCCS or force CAS to become unclassified.

Interview Questions

1. What requirements will an interface method have to meet in order to provide real time interaction between DSACS and CAS?

2. Do interface methods currently exist which allow for real time interactive secure transmission of data between dissimilar systems?

a. If no, what is lacking?

b. If yes, briefly describe.

3. Can these requirements be met with CAS remaining classified within WWMCCS?

a. If yes, how?

b. If no, why?

4. Can these requirements be met with DSACS remaining unclassified?

a. If yes, how?

b. If no, why?

5. Could an existing interface be used to interface CAS and DSACS?

a. If yes, what needs to be done in order to implement this method?

b. If no, why?

6. Are there any developments being planned or in progress for a new interface method which would provide a solution to this problem?

a. If yes, describe the developments.

b. How long before they could be implemented?

c. Could these developments lead to expanded capabilities at a later date?

7. If no interface currently exists or is being developed to meet the needs of CAS and DSACS suggest what the Air Force should do.

Appendix B: List of Participating Respondents

	NAME	ADDRESS	TELEPHONE
1.	Fred Campbell	AFLC-LOC/OOW Wright-Patterson AFB OH	AV787-7784
2.	Capt Lucky Goebel	AFLMC/LGY Gunter AFS AL	AV446-3514
3.	Jim Gordy	JDSSC/C323 Pentagon Washington DC	AV225-0568
4.	Capt Thomas James	AFLMC/LGY Gunter AFS AL	AV446-4524
5.	Herman Stein	JDSSC/C321 Pentagon Washington DC	AV227-5762
6.	Major Ian Birdsal	AFLC-LOC/CFM Wright-Patterson AFB OH	AV787-4939
7.	MSgt Paul Scott	AFLC-LOC/CFM Wright-Patterson AFB OH	AV787-4939
8.	Dean Reesey	OJCS/C3SCI Pentagon Washington DC	AV225-6326
9.	Capt Joe Itze	ESD/ALSE Hanscom AFB MA	AV487-4915
10.	Don Miller	HQ AFLC/DCT Wright-Patterson AFB OH	AV787-4958
11.	Marv Richardson	HQ AFLC/DCT Wright-Patterson AFB OH	AV787-4958

	NAME	ADDRESS	TELEPHONE
12.	Don Zimmerman, VP	Synergy Inc. Washington DC	202-232-6261
13.	Harold Folts	Omnicom Inc. Vienna VA	703-281-1135
14.	Al Speed	1st ISG/TPRS Pentagon Washington DC	202-695-6543
15.	Dick Neil	Honeywell Inc. McLean VA	703-827-3702
16.	Ray Denenberg	Library of Congress Washington DC	202-287-5894
17.	Richard Cavedo	NCR Comten Inc. Rockville MD	301-340-8220
18.	Dr. Anupam Shah	Computer Sciences Corp. Falls Church VA	703-237-2000
19.	Major Brad Christie	HQ USAF/LEYW Pentagon Washington DC	AV227-6984
20.	Major Aaron DeWispelare	AFLMC/LGY Gunter AFS AL	AV446-4524
21.	Jim DeGroff	ASPO/PGD Gunter AFS AL	AV446-4074
22.	Major Mike Allen	HQ DCA Washington DC	AV356-5025
23.	Linda Heckman	Mitre Corp. McLean VA	703-883-7312

	NAME	ADDRESS	TELEPHONE
24.	Carl Driscoll	Cincom Systems Inc. Fairfax VA	703-352-4482
25.	John Landwehr	Savings & Loan Data Corp Cincinatti OH	513-489-6580
26.	Bill Post	Verdix Corp. McLean VA	703-448-1980
27.	Dr. Sam Steppel	Computer Sciences Corp. Falls Church VA	703-237-2000
28.	Donald J. Yeskey	DOD CSC Ops System Eval Fort Meade MD	301-859-6993

Appendix C: Determination of Alternatives

The determination of how many and what alternative interface methods exist is a subjective decision which is based upon the relationship of the information gathered in the findings of the interviews with the selection criteria. These decisions were based upon the following factors associated with the selection criteria:

1. Time to implement the alternative. An alternative may very well exist for each of the three time periods (short - less than 2 years, medium - 2 to 5 years, and long - greater than 5 years) assuming that the combination of other selection factors are significantly different.

2. Interoperability. This term is defined as "the capability of two or more items or components of equipment to perform essentially the same function or to complement each other in a system regardless of differences in technology" (25:363). Alternative interface methods will be chosen based upon the system's possession of an on-line capability, its ability to process formatted or unformatted inquiries, its ability to perform batch processing and to avoid man/machine interaction. Any attributes of a system which affect the interactiveness of the DSACS and CAS interface may help characterize an alternative.

3. Security. Various alternatives exist depending upon whether or not an interface must operate entirely at one level of security classification or is capable of interfacing systems at different levels of security classification. The specific level of security required for the operation of the interface is an important factor. The ability of an interface to filter, screen and provide an audit of transactions will help discriminate between various alternatives.

4. Expandability. An alternative interface method may be distinquished from others based upon the potential for new technologies and networking to be incorporated into the

interface system.

5. Permanence. An alternative can be distinquished from others of seemingly equal worth based upon the potential and possibility of the interface being a permanent solution to the problem. An assessment of the newest developing technologies and trends in Air Force and Army computer security policy may help to determine the potential permanence of a solution.

6. Real Time. This term is defined as "The absence of delay, except for the time required for the transmission by electromagnetic energy between the occurrence of an event or transmission of data and the knowledge of the event, or reception of the data at some other location" (25:568).

Appendix D: Secure Communications Processor

The Secure Communications Processor (SCOMP) is a mid-range Honeywell DPS 6 sixteen bit mini-computer designed to provide internal computer multilevel security protection for sensitive and classified data. The SCOMP features:

1. Eight hierarchical levels of security or privacy and thirty-two mutually independent security categories that protect data from unauthorized access.

2. Eight levels of integrity and thirty-two mutually independent categories, that protect information from unauthorized modification.

3. An access control list (ACL) which specifies who has read, write and execute permissions.

4. Extensive security auditing.

5. A Trusted Computer System designed to a Formal Top Level Specification ... which has been validated by the DOD Computer Security Center ... as a Class A1 (the highest security category system available with current technology) (36,57).

The Honeywell SCOMP hardware is a modification of the standard Honeywell DPS 6. The standard Central Processing Unit (CPU) was modified, a Security Protection Module (SPM) and a Virtual Memory Interface Unit (VMIU) were added to the original hardware. The SPM resides between the modified CPU and all other system elements and captures all processor requests and performs all required mediation before accessing memory or input/output devices.

The system software is called the SCOMP Trusted Operating Program (STOP). STOP consists of three components: a security kernel, a trusted computer base, and a kernel interface package.

The security kernel performs "all resource management, process scheduling, memory management, trap and interrupt management, and auditing". The kernel also controls access to data according to an embedded security policy (63:189).

The trusted computer base (TCB) provides all the security mechanisms and applications interfaces for this multi-user operating system. The TCB provides an interface to the SCOMP system for the user, provides the system operator with the capability to run the system and provides the system administrator with the capability to maintain the system (63:189-191,36).

The SCOMP kernel interface package (SKIP) provides an interface to the secure environment which allows the users to interface applications and systems with the security mechanisms of the SCOMP system. The SKIP provides the user with a hierarchical file system, a process control mechanism and support device for inputs and outputs (63:191,36).

The SCOMP can be applied as a stand alone (host), a secure front-end processor and as a network guardian in communication networks (36).

Appendix E: The ACCAT Guard

The Advanced Command and Control Architectural Testbed (ACCAT) Guard, sponsored by the Naval Electronics System Command (NAVELEX) and developed by Logicon Inc., was designed to use security kernel technology to allow controlled information exchanges between a Top Secret/Sensitive Compartmented Information computer network and a Secret computer network. The ACCAT Guard is able to handle data base queries, replies and mail from either system.

The ACCAT Guard uses human review to regulate information flowing from one system to the other. Sanitation Personnel (SP's) "edit all high-to-low messages to remove sensitive data," and "translate all English language data base queries (high-to-low or low-to-high) to a canonical form acceptable by the data base software". The Security Watch Officer (SWO) "reviews all high-to-low data before it can be sent to the low side." Once the SP's have sanitized the data, it is sent to the SWO before being released to the low side. "Low-to-high queries, replies, and user mail require no action, except that the English-language queries are translated to canonical form by the SP" (8:3-4).

The ACCAT Guard is currently being implemented using the SCOMP system (63:192). See Appendix D.

Appendix F: The FORSCOM Security Monitor

The U.S. Army Forces Command (FORSCOM) Security Monitor (FSM) was developed by Logicon Inc., and sponsored by Navy Electronics System Command (NAVELEX) and the Defense Communication Agency (DCA) to act as a mediator between the FORSCOM Honeywell 6000 host computer and its remote terminals.

FORSCOM's Honeywell 6000 computer is part of the Top Secret WWMCCS Interactive Network (WIN). All WIN remote terminals are required to operate at a Top Secret Level (39:3-2-1). The FSM was developed to allow some of the remote WIN terminals to operate at a lower Secret level by using three security mechanisms to protect against unauthorized information flows. These mechanisms are automatic screening, human screening and filtering.

The FSM performs automatic screening for outputs leaving the Top Secret H6000 which conform to a fixed format. These outputs are recognized by the FSM and are sent to the user without human review. However, the number of outputs which can be automatically screened is limited over a given time period. Excess outputs during the time period must pass a human review.

Human review is reserved for outputs from the higher security level with a variable format and for excess fixed

formats. A person must screen the outputs for any data which is too sensitive to be viewed by the user.

A filter mechanism is used on outputs from the lower security level remotes destined for the higher security level. The filter insures that no sequence of low side commands could possibly destroy data, deny service, or elicit sensitive information from the H6000. The filter also checks file names to insure that the user has the proper permission to access them.

In addition to the three security mechanisms mentioned above, the FSM can audit transactions to help monitor its performance (8:6-8).

Currently SCOMP is the hardware that Army is implementing on the FORSCOM Security Monitor (63:192). See Appendix D.

Appendix G: The Large Scale Integration Guard

The Large Scale Integration (LSI) Guard was sponsored by the Navy Electronics Systems Command (NAVELEX) and developed by I. P. Sharp Associates to be a stand-alone system using off-the-shelf components for a variety of applications.

> The LSI Guard is a microprocessor guard system, completely contained in a single video terminal. The user can connect to either the high or the low side as a normal terminal user, or can act as a review officer for data moving between the two (8:9).

The LSI Guard can only support one user at a time, but a number of users can be authorized to use it as long as they log on at different times. "The Terminal System Security Officer (TSSO) may add or delete LSI Guard users, or modify current users' identification numbers, passwords, and privileges" (8:10).

A user can perform a downgrade function when sending information from the higher security level to the lower security level. Each output message must be viewed one at a time on the screen and released, rejected, or saved by the user. The LSI Guard has the ability to audit all transactions and all text before and/or after editing for downgrade (8:10).

Appendix H: The Korean Air Intelligence System

The Korean Air Intelligence System (KAIS) is sponsored by the U.S. Air Force Pacific Air Command (PACAF) and the Rome Air Development Center, Griffiss AFB NY. The Security Interface portion of the KAIS is being developed by Computer-Tek Inc.

The KAIS Security Interface is designed to process intelligence data between two untrusted computer systems which are run at different security levels. The objective of the interface is to provide a more timely mechanism to move data between the two levels. Specifically, the KAIS system is intended to avoid the slow process of dumping highly classified data on to magnetic tapes for manual review before sending data to users at lower levels of security.

In an effort to avoid the use of tapes, one suggested design calls for the positioning of a processor at each computer security level interface within the system. As low security messages enter the higher security level a non-forgeable authenticator would be attached to the message. As messages exit the high security level the authenticator is re-computed. If the authenticator has not been altered by the addition of unauthorized data, the high side is allowed to automatically release the message to the low side. All other high-to-low traffic would be manually reviewed prior to

release. All low-to-high messages will be reviewed prior to release to the high side (8:12-13).

Appendix I: The Restricted Access Processor

The Restricted Access Processor (RAP) is sponsored by the National Aeronautics and Space Administration (NASA) and is being developed by Computer Sciences Corp. (CSC), and Sytek Inc. to support NASA's Network Control Center (NCC). The NCC has a requirement to support classified DOD missions as well as unclassified world-wide commercial missions. The RAP, Phase II of NASA's Ground System Security Upgrade, was designed to protect classified DOD mission data without causing disruption to the NCC's ability to support commercial missions (8:16-17).

> The RAP processes both NCC input messages and NCC output messages by examining the fields in each message to determine the source, the destination, and the function of the message. Only messages containing valid headers and subfields, as indicated in the RAP data base, are forwarded; other messages cause an operator alert (8:17).

> The security of the RAP is established by an implementation of both hardware and software. The security critical message processing software is isolated and defined within a security perimeter for verification. The boundary of the security perimeter is also enforced by a hardware separation of functions in a multi microprocessor architecture. CSC is applying state of the art verification techniques to the software within the security perimeter (59,62).

Appendix J: The Defense Data Network

Policy

In April 1982, the DOD directed that the Defense Data Network (DDN) be implemented as the DOD common-user data-communications network. Office of the Secretary of Defense Policy issued 10 March 1983 stated:

> All DOD ADP systems and data networks requiring data communications services will be provided long-haul and area communications, interconnectivity, and the capability for interoperability by the DDN (18:1).

Description

The DDN is a packet-switching network designed to meet the data communications requirements of the DOD (18:3).

Packet switching is a method for handling data as it is transmitted through a communications network. The switching nodes to which subscriber computers are attached subdivide information streams into small packets, then route and otherwise handle each packet as if it were a separate message (18:1). (See Figure 5).

Each packet switch is a current generation computer designed for unattended operation, easy maintenance, and compatibility with existing [Advanced Research Projects Agency Network] ARPANET Interface Message Processor (IMP) packet switching software (18:3).

The DDN is composed of two backbone network segments. One segment [containing the Military Network (MILNET) and ARPANET] is unclassified, the other is classified. User traffic on the unclassified network will be protected by commercial encryption techniques using the Data

Encryption Standard (DES) on [continental U.S.] CONUS inter-switch trunks. ...In the classified network all data and related control functions are protected by military-grade encryption devices (18:7).

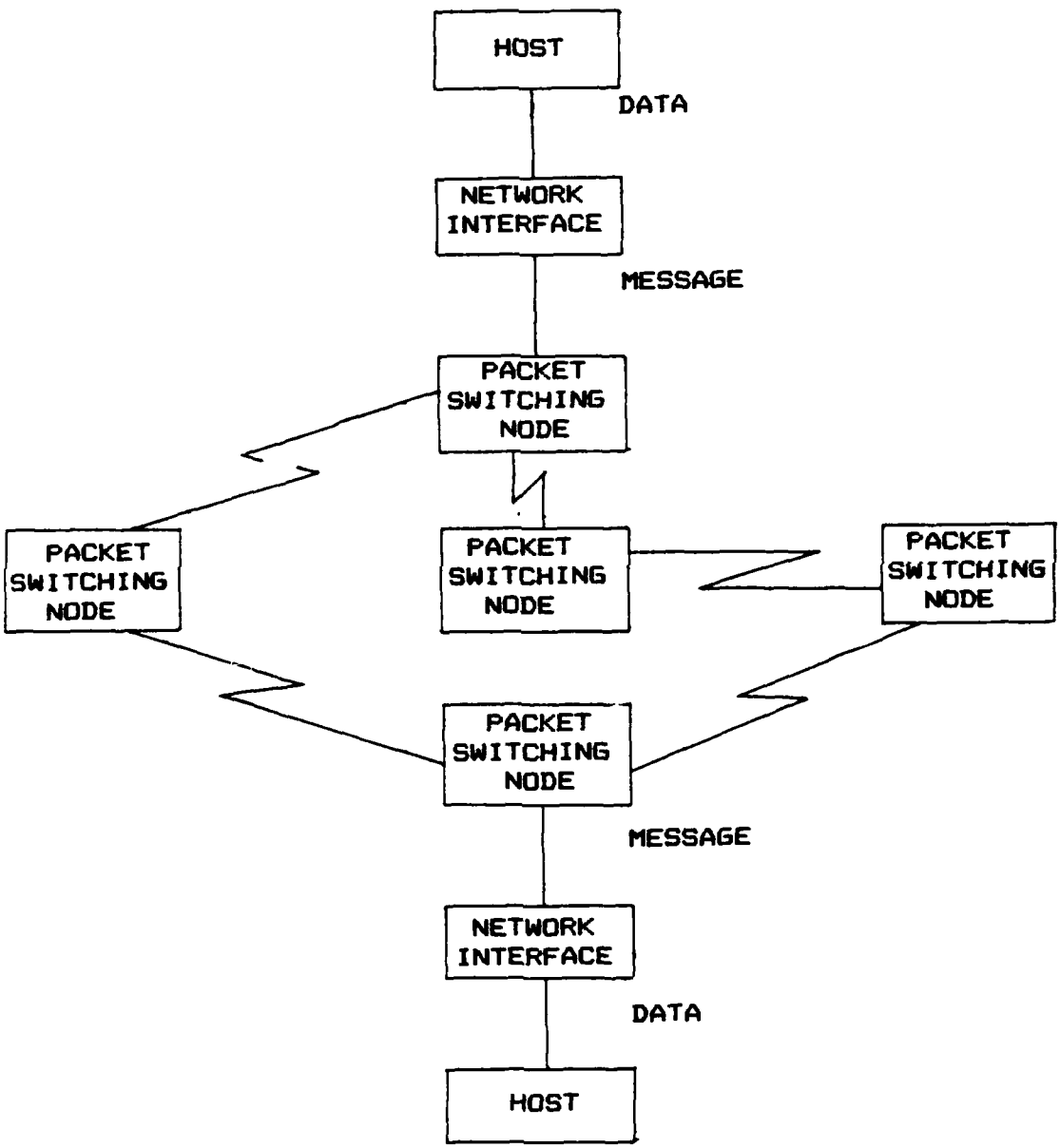


Figure 5. A Packet Switching Network (18:1)

Over the next few years, as end-to-end encryption (E3) security devices become available, the [DOD Intelligence Information System] DODIIS, [Strategic Air Command Digital Network] SACDIN, [WWMCCS Intercomputer Network Communications Subsystem] WINCS, and other Top Secret subscribers will be integrated with the SECRET backbone, forming the classified segment of the DDN (18:3). See Figure 6.

In order to permit classified users to exploit the large bandwidth of the unclassified segment of DDN, the classified and unclassified DDN segments will be interconnected using one-way network gates (switch level gates). This will result in establishing the segmented DDN [Figure 7] (18:3).

Finally the availability of the [National Security Agency] NSA developed BLACKER equipment will allow the segmented DDN to be integrated into a single, shared, multilevel secure network, and will allow the InterService/Agency Automatic Message Processing Exchange (I-S/AMPE) subnetwork and other multilevel secure hosts to use the DDN as a backbone (18:3).

Access

> Each subscriber access line to the classified DDN segment will operate at a single system-high security level, for example Secret, or Top Secret. ... End-to-end encryption devices will separate the traffic of different security levels or communities of interest. ... Thus, through end-to-end encryption techniques, each network user will be able to communicate only with other users belonging to the same subscriber community (18:8).

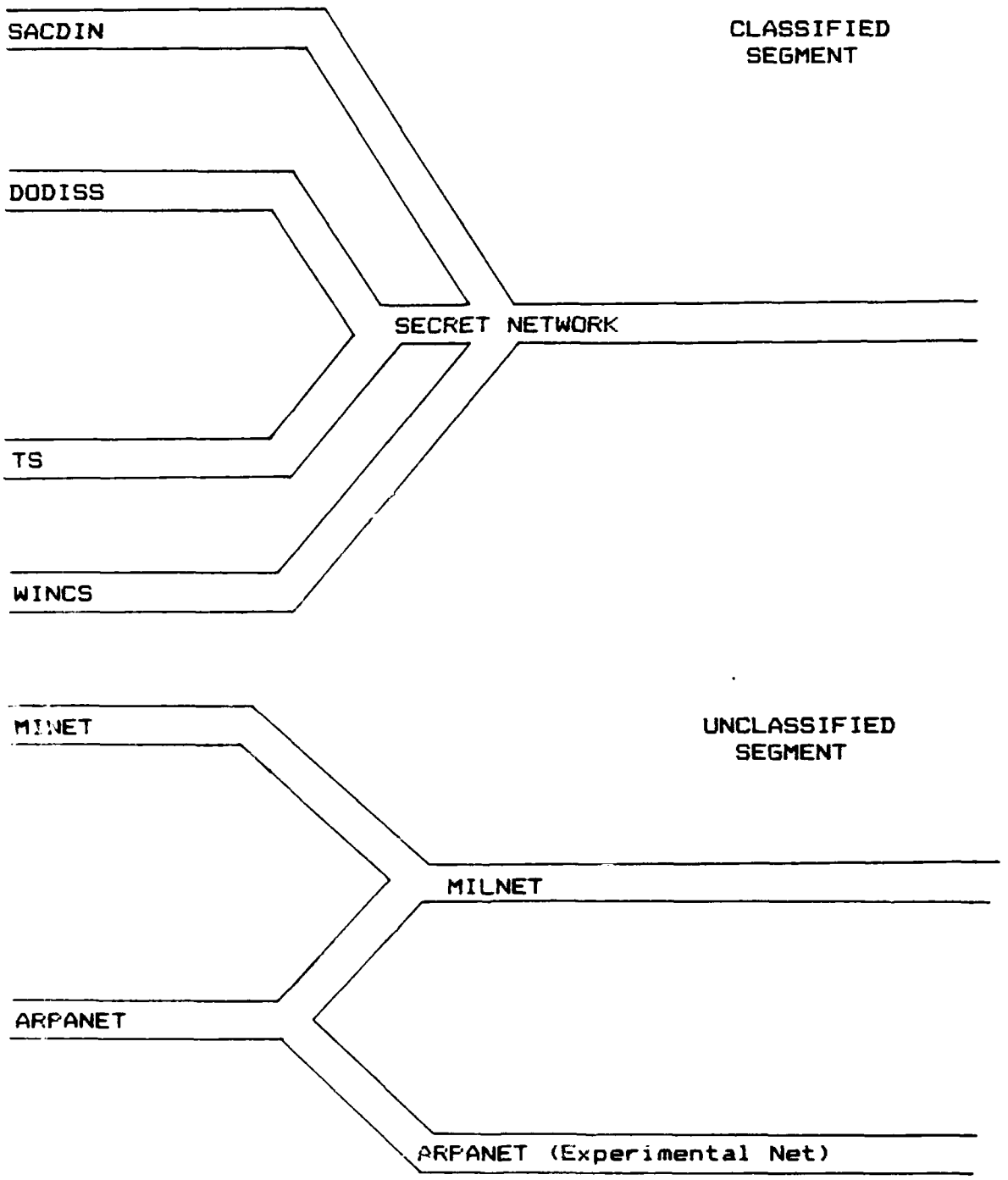


Figure 6. DDN Evolutionary Strategy (18:3)

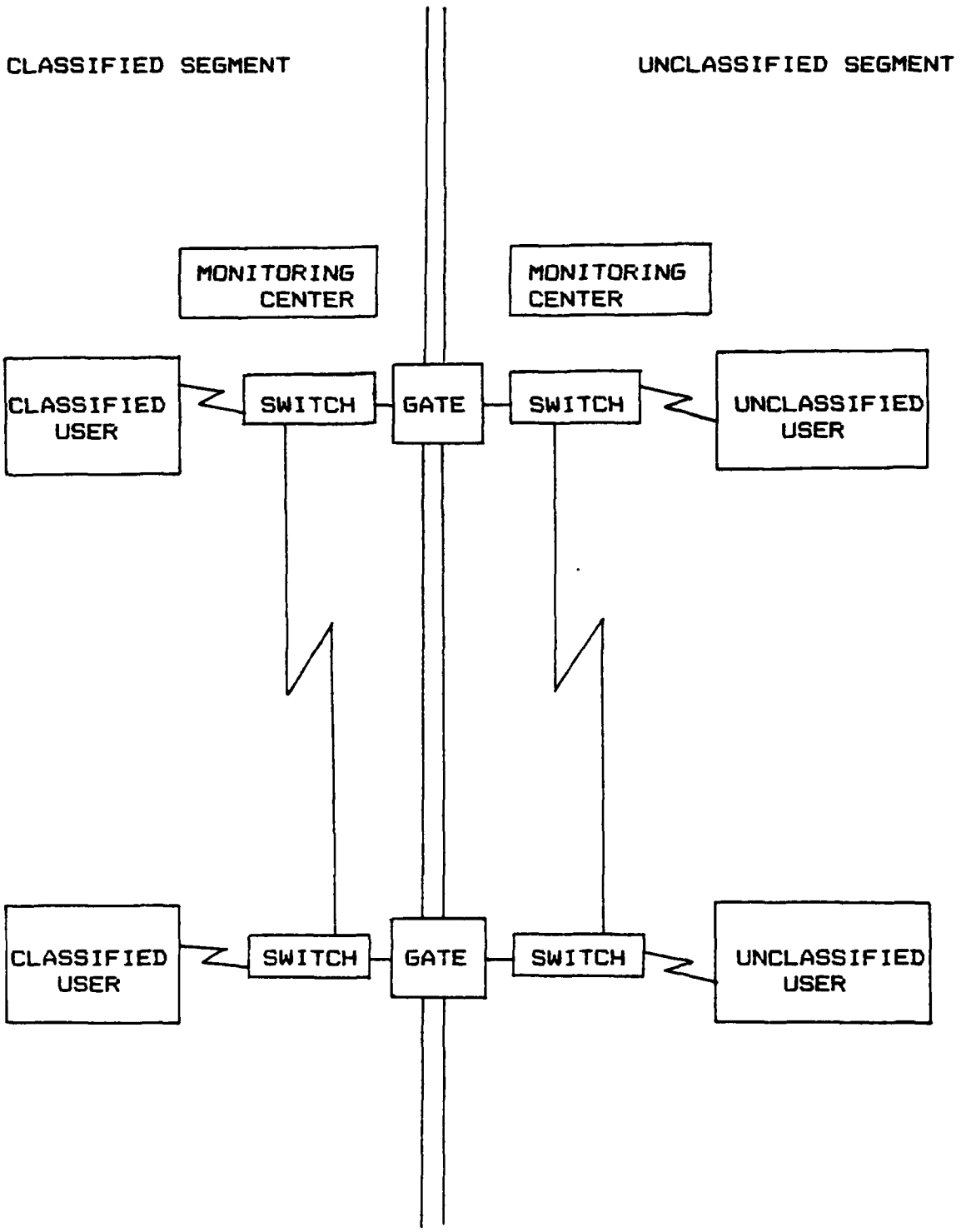


Figure 7. Segmented DDN (18:7)

Appendix K: Unclassified Parallel Interface

The basic purpose of an unclassified parallel interface between DSACS and CAS would be to circumvent the requirement to operate on a multilevel secure mode. The various descriptions given during the interviews can best be categorized as a "generic" methods.

Very basically, the Air Force could remove unclassified data resident within the CAS which has been determined to be essential for transmission to DSACS. This data would be placed in an unclassified minicomputer not directly connected to CAS. The unclassified data in the minicomputer could be updated as often as needed with the latest changes from CAS using magnetic tapes. The minicomputer would be able to to update DSACS immediately as soon as the tape transfer was complete. DSACS could update the minicomputer's data on a real-time basis (6,47).

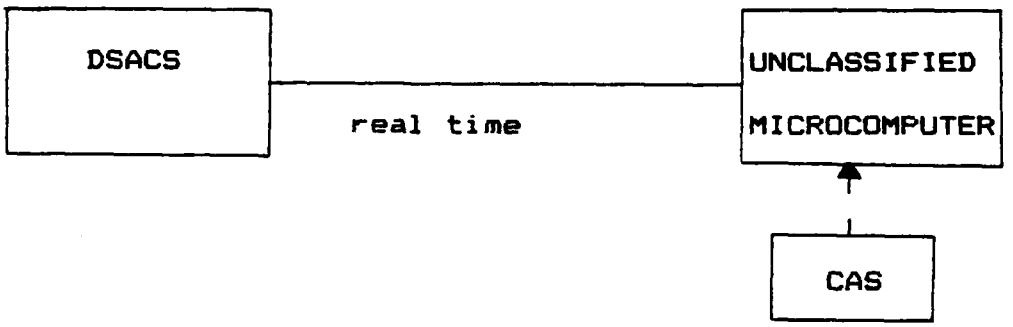


Figure 8. An Unclassified Parallel Interface

Appendix L: Trusted Computer System Evaluation Criteria

Division D: Minimal Protection. This division contains only one class. It is reserved for those systems that have been evaluated but fail to meet the requirements for a higher evaluation class.

Division C: Discretionary Protection. Classes in this division provide for discretionary (need-to-know) protection and accountability of subjects and the actions they initiate, through the inclusion of audit capabilities.

Class C1: Discretionary Security Protection. The TCB of Class C1 systems nominally satisfies the discretionary security requirements by providing separation of users and data.

Class C2: Controlled Access Protection. Systems in this class enforce a more finely grained discretionary access control than class C1 systems, making users individually accountable for their actions through logic procedures, auditing of security-relevant events, and resources encapsulation.

Division B: Mandatory Protection. The notion of a TCB that preserves the integrity of sensitivity labels and uses them to enforce a set of mandatory access control rules is a major requirement in this division. Systems in this division must carry the sensitivity labels with major data structures in the system. The system developer also provides the security policy model on which the TCB is based and furnishes a specification of the TCB. Evidence must be provided to demonstrate that the reference monitor concept has been implemented.

Class B1: Labeled Security Protection. Class B1 systems require all the features required for class C2. In addition, an informal statement of the security policy model, data labeling, and mandatory access control over named subjects and objects must be present. The capability must exist for accurately labeling exported information. any flaws identified by testing must be removed.

Class B2: Structured Protection. In class B2 systems, the TCB is based on a clearly defined and documented formal security policy model that requires the discretionary and mandatory access control enforcement found in the B1 systems be extended to all subjects and objects in the system. In addition, covert channels are addressed. The TCB must be carefully constructed into protection-critical elements. The TCB interface is well defined and the TCB design and implementation enable it to be subjected to more thorough testing and more complete review. Authentication mechanisms are strengthened, trusted facility management is provided in the form of support for systems administrator and operator functions, and stringent configuration management controls are imposed. The system is relatively resistant to penetration.

Class B3: Security Domains. The class B3 TCB must satisfy the reference monitor requirements that it mediate all accesses of subjects to objects, be tamperproof, and be small enough to be subjected to analysis and tests. To this end, the TCB is structured to exclude code not essential to security policy enforcement, with significant software engineering during TCB design and implementation directed toward minimizing its complexity. A security administrator is supported, audit mechanisms are expanded to signal security-relevant events, and system recovery procedures are required. The system is highly resistant to penetration.

Division A: Verified Protection. This division is characterized by the use of formal security verification methods to assure that the mandatory and discretionary security controls employed in the system can effectively protect the classified and other sensitive information stored or processed by the system. Extensive documentation is required to demonstrate that the TCB meets the security requirements in all aspects of design, development, and implementation.

Class A1: Verified Design. Systems in class A1 are functionally equivalent to those in class B3 in that no additional architectural features or

policy requirements have been added. The distinguishing feature of systems in this class is the analysis derived from formal design specification and verification techniques and the resulting high degree of assurance that the TCB is correctly implemented. This assurance is developmental in nature starting with a formal model of security policy and a formal top-level specification (FTLS) of the design. In keeping with the extensive design and development analysis of the TCB required of systems in class A1, more stringent configuration management is required and procedures are established for securely distributing the system to sites. A system security administrator is supported (60:26-29).

Appendix M: Glossary of Terminology

Access

A specific type of interaction between a subject and an object that results in the flow of information from one to the other (19:109).

Approval/Accreditation

The official authorization that is granted to an ADP system to process sensitive information in its operational environment, based upon comprehensive security evaluation of the system's hardware, firmware, and software security design, configuration and implementation, and of the other system procedural, administrative, physical, TEMPEST, personnel, and communications security controls (19:109).

Audit Trail

A set of records that collectively provide documentary evidence of processing used to aid in tracing from original transactions forward to related records and reports, and backwards from records and reports to their component source transactions (19:109).

Certification

The technical evaluation of a system's security features, made as part of and in support of the approval/accreditation process, that establishes the extent to which a particular computer system's design and implementation meet a set of specified security requirements (19:110).

Controlled Security Mode

A mode of operation where internal security controls prevent inadvertent disclosure. Personnel, physical and administrative controls prevent delibrate, malicious attempts to gain unauthorized access. A system that operates in the

controlled security mode may service both cleared and uncleared users. If required, it may concurrently service both secured and unsecured remote terminal areas (24:17).

Custodial Accountability

The maintenance of data in the wholesale conventional ammunition inventory record to reflect the receipt, issue balance, and other quantitative and financial data determined by the SMCA as the minimum essential for the proper control and management of Military Services stocks in storage (12:encl 2).

Dedicated Security Mode

A mode of operation where the automated data processing systems (ADPS), its peripherals, and remotes are exclusively used and controlled by specific users or groups of users to process a particular type and category of classified or sensitive material. All users of the system must have clearances and a need-to-know for all material in the ADPS (24:17)

Designated Approval Authority

A designated [Air Force] official who approves the operation of automatic data processing systems at the automatic data processing facilities under his or her jurisdiction for storage of classified or sensitive unclassified information or for critical processing (24:17).

Each MAJCOM or [Separate Operating Agency] SOA commander is the designated approving authority (DAA) for that command or agency (24:4).

Financial Accountability

The maintenance by the responsible Military Services of summary financial data for transactions and inventory balances to provide the minimum essential basis for controlling, financing, planning, programming, and budgeting of items in

the wholesale conventional ammunition inventory (12:encl 2).

Formal Proof

A complete and convincing mathematical argument, presenting the full logical justification for each proof step, for the truth of a theorem or set of theorems. The formal verification process uses formal proofs to show the truth of certain properties of formal specification and for showing that computer programs satisfy their specifications (19:111).

Formal Security Policy Model

A mathematically precise statement of a security policy. To be adequately precise, such a model must represent the initial state of a system, the way in which the system progresses from one state to another, and a definition of a "secure" state of the system. To be acceptable as a basis for a [trusted computing base] TCB, the model must be supported by a formal proof that if the initial state of the system satisfies the definition of a "secure" state and if all assumptions required by the model hold, then all future states of the system will be secure (19:111).

Formal Verification

The process of using formal proofs to demonstrate the consistency (design verification) between a formal specification of a system and a formal security policy model or (implementation verification) between the formal specification and its program implementation (19:111).

Multilevel Security Mode

A mode of operation that provides a capability for various levels and categories or compartments of data to be concurrently stored and processed in an automated data processing system and permits selective access to such material concurrently by users who have differing security clearances and

need-to-know. Internal controls, as well as personnel, physical, and administrative controls, separate users and data on the basis of security clearance and need-to-know. The internal security controls must be thoroughly demonstrated to be effective in preventing delibrate malicious attempts to gain unauthorized access to classified information. Depending on the constraints the Designated Approving Authority (DAA) places on the system, this mode of operation can accomodate the concurrent processing and storage of two or more levels of classified data, or one or more levels of classified data with unclassified data (24:17).

Reference Monitor Concept

An access control concept that refers to an abstract machine that mediates all access to objects by subjects (19:112).

Retail Conventional Ammunition

Conventional munition stocks between point of receipt at first retail [continental United States] CONUS activity and the point of consumption (12:encl 2).

Security Kernel

The hardware, firmware, and software elements of a Trusted Computing Base that implement the reference monitor concept. It must mediate all accesses, be protected from modification, and be verifiable as correct (19:113).

Secure kernels are small, isolated portions of the operating system that perform the system's basic operations in a provably correct manner. This concentrates the key system protection mechanism (process creation and execution, and mediation of primary interrupts and responses) into a totally reliable segment of the system, rather than dispersing them throughout the software. Secure operating systems can then be built around these kernels (4:132).

System High Security Mode

A mode of operation when all personnel with access to the automated data processing system (ADPS) have a security clearance, but not a need-to-know for all the material then contained in the system. An ADPS is operating in the system high security mode when the central computer facility and all of its connected peripheral devices and remote terminals are protected according to the requirement for the highest classification of material contained in the system. In this mode, the ADPS design and operation must accordingly provide for some internal control of concurrently available classified material in the system on the basis of need-to-know (24:19).

Trusted Computer System

A system that employs sufficient hardware and software integrity measures to allow its use for processing sensitive information (19:114).

Trusted Computing Base (TCB)

The totality of protection mechanisms within a computer system - including hardware, firmware, and software - the combination of which is responsible for enforcing a security policy. It creates a basic protection environment and provides additional user services required for a trusted computer system. The ability of a trusted computing base to correctly enforce a security policy depends solely on the mechanisms within the TCB and on the correct input by system administrative personnel of parameters (e.g. a user's clearance) related to the security policy (19:114).

Wholesale Conventional Ammunition

All conventional ammunition stocks between point of production and point of receipt at the first retail CONUS activity (such as tidewater port, air base, post, camp or station) (12:encl 2).

BIBLIOGRAPHY

1. Allen, Maj Mike, HQ Defense Communications Agency. Telephone interview. Washington DC, 12 June 1985.

2. Bedau, Hugo, A., and others. Making Decisions - A Multidisciplinary Introduction. Reading: Addison-Wesley Publishing Co., 1981.

3. Birdsal, Maj Ian, Munitions Staff Officer. Written reply to interview questions. HQ AFLC Logistics Operations Center/CFM, Wright-Patterson AFB OH, 16 May 1985.

4. Buck, Edward R. Introduction to Data Security and Controls. Q.E.D. Information Sciences Inc., Wellesley MA, 1982.

5. Campbell, Fred, HQ AFLC Logistics Operations Center WWMCCS ADP System Security Officer. Telephone interview. Wright-Patterson AFB OH, 6 June 1985.

6. Caveto, Richard, Regional Technical Manager, Federal Region. Telephone interview. NCR Comten Inc., Rockville MD, 30 May 1985.

7. Cheheyl, M. H., Computer Science Researcher. Telephone interview. MITRE Corp., Bedford MA, 9 July 1985.

8. Cheheyl, M. H., "Security Guards." WP-24472, MITRE Corp., Bedford MA, October 1982.

9. Christie, Maj Brad, Supply Staff Officer. Telephone interview. HQ/LEYW, Pentagon, Washington DC, 24 July 1985.

10. Comptroller General of the United States. "Centralized Ammunition Management -- A Goal Not Yet Achieved." LCD 80-1. Washington: U.S. General Accounting Office, 26 November 1979.

11. Comptroller General of the United States. "Effective Central Control Could Improve DOD's Ammunition Logistics." B-176139. Washington: U.S. General Accounting Office, 6 December 1973.

12. Czapliki, Edward J., and others. The Single Manager for Conventional Ammunition: Another Look. Research Report AD - A138 216. Industrial College of the Armed Forces, Fort Lesley J. McNair, Washington DC, May 1983.

13. DeGroff, Jim, ASPO/PGD. Telephone interview. Gunter AFS AL, 12 June 1985.

14. Denenberg, Ray, NDMSO Processing. Telephone interview. Library of Congress, Washington DC, 6 June 1985.

15. Department of Defense. ADP Security Manual. DOD 5200.28M, January 1973.

16. Department of Defense. Briefing Slides of the Defense Standard Ammunition Computer System In-process Review to The Joint Logistics Systems Review Committee, 9 November 1983.

17. Department of Defense. Computer Security Requirements - Guidance for Applying Department of Defense Trusted Computer System Evaluation Criteria in Specific Environments. CSC-STD-003-85. DOD Computer Security Center, 25 June 1985.

18. Department of Defense. Defense Data Network. Product Description. Defense Communications Agency. Publication received from HQ AFLC/DCT, Wright-Patterson AFB OH, undated.

19. Department of Defense. Department of Defense Trusted Computer System Evaluation Criteria. CSC-STD-001-83. DOD Computer Security Center, 15 August 1983.

20. Department of Defense. Report on the Audit of the Single Manager for Conventional Ammunition Program. Research Report LD - 59050A. Office of the Inspector General for Auditing, Arlington VA, June 1984.

21. Department of Defense. Security Requirements for Automatic Data Processing (ADP) Systems. DODD 5200.28, 18 December 1972.

22. Department of Defense. Single Manager for Conventional Ammunition. DOD Directive 5160.65. Washington: Government Printing Office, 17 November 1981.

23. Department of Defense. Technical Rationale Behind CSC-STD-003-85 Computer Security Requirements. CSC-STD-004-85. DOD Computer Security Center, 25 June 1985.

24. Department of the Air Force. Automatic Data Processing (ADP) Security Policy, Procedures and Responsibilities. AFR 205-16, 1 August 1984.

25. Department of the Air Force. Compendium of Authenticated Systems and Logistics Terms, Definitions and Acronyms. AU-AFIT-LS-3-81. Air Force Institute of Technology, Wright-Patterson AFB OH, 1981.

26. Department of the Air Force. Defense Standard Ammunition Computer System Service Requirements - U.S. Air Force. Airmunitions Management Division, Air Logistics Center, Hill AFB UT. July 1983.

27. Department of the Army. Joint Services System Functional Requirements Statement for the Defense Standard Ammunition Computer System. Headquarters U.S. Army Armament, Munitions and Chemical Command. 15 November 1984.

28. DeWispelare, Maj Aaron, Ph.D. Scientific Analyst. Telephone interview. AFLMC/LGY, Gunter AFS AL, 10 June 1985.

29. Driscoll, Carl, District Technical Network Management Specialist. Telephone interview. Cincom Systems Inc., Fairfax VA, 16 July 1985.

30. Emory, William C. Business Research Methods. Homewood: Richard D. Irwin, Inc., 1980.

31. Folts, Harold, Computer Systems Analyst. Telephone interview. Omnicom Inc., Vienna VA, 10 June 1985.

32. Goebel, Capt Lucky A., Scientific Analyst. Telephone interview. AFLMC/LGY, Gunter AFS AL, 21 May 1985.

33. Gordy, Jim, Systems Analyst, Joint Data Systems Support Center. Telephone interview. Pentagon, Washington DC, 20 May 1985.

34. Headquarters Air Force Logistics Command. Message R151900Z Jul 83 From HQ AFLC/LOW to Directorate of Materiel Management Hill AFB/MMW, Subject: Draft Functional Description - Defense Standard Ammunition Computer System.

35. Heckman, Linda, Researcher. Telephone interview. MITRE Corp, McLean VA, 7 June 1985.

36. Introducing the Honeywell Secure Communications Processor. Product Description. Honeywell Information Systems, Federal Systems Division, McLean VA, undated.

37. Itze, Capt Joe, ESD/ALSE. Telephone interview. Hanscom AFB MA, 30 May 1985.

38. James, Capt Thomas G., Computer Analyst. Telephone interview. AFLMC/LGY, Gunter AFS GA, 30 May 1985.

39. Joint Chiefs of Staff. WWMCCS ADP System Security (WASS) Manual. JCS Pub 22, January 1980.

40. Koistinen, Paul A. C. The Military-Industrial Complex: A Historical Perspective. New York: Praeger Publishers, 1980.

41. Landwehr, John, Customer Operations. Telephone interview. Savings and Loan Data Corp, Cincinatti OH, 7 June 1985.

42. Legare, Greg. "Air Force/HQ AMCCOM Communication Security." Minutes of 22 January 1985 Conference. Headquarters, U.S. Army Armament, Munitions and Chemical Command, Rock Island IL.

43. Legare, Greg, Product Manager, Defense Standard Ammunition Computer System. Telephone interview. Headquarters US Army Armament, Munitions and Chemical Command, Rock Island IL, 25 March 1985.

44. Logistics Management Institute. Condition and Operation of DOD Ammunition Production Facilities - Phase II. Task 68-19, Vol I, Defense Contract No. SD-271, Report AD-711 607, July 1970.

45. McNamara, Ralph, Assistant Chief, Airmunitions Requirements and Distribution Branch. "Air Force Combat Ammunition System." Briefing to the Product Manager, Defense Standard Ammunition Computer System, 22 January 1985. Directorate of Materiel Management, Air Logistics Center, Hill AFB UT.

46. McNamara, Ralph, Assistant Chief, Airmunitions Requirements and Distribution Branch, Directorate of Materiel Management. Telephone interview. Ogden Air Logistics Center, Hill AFB UT, 29 March 1985.

47. Miller, Don, DDN Spokesman. Telephone interview. HQ AFLC Directorate of Communications and Electronics, Technology and Integration Division, Wright-Patterson AFB OH, 22 May 1985.

48. Neil, Dick, Computer Systems Analyst. Telephone interview. Honeywell Inc., McLean VA, 10 June 1985.

49. Partner, Mildred, PhD. Surveys, Polls, and Samples: Practical Procedures, New York: Cooper Square Publishers Inc., 1966.

50. Post, Bill, Computer Systems Analyst. Telephone interview. Verdix Corp, McLean VA, 12 June 1985.

51. Reesey, Dean, Office of the Joint Chiefs of Staff. Telephone interview. Pentagon, Washington DC, 11 June. 1985.

52. "Restricted Access Processor Program: Provably Secure Communications for NASA's Space Programs." Computer Sciences Corp. Briefing to HQ SAC, Omaha NE, 29 May 1985.

53. Richarson, Marv, HQ AFLC/DCT. Telephone interview. Wright-Patterson AFB OH, 7 June 1985.

54. Scott, MSgt Paul, Munitions Staff NCO. Written reply to interview questions. Logistics Operations Center/CFM Wright-Patterson AFB OH, 16 May 1985.

55. Shah, Anupam, Dr., Senior Member Executive Staff, Systems Division. Telephone interview. Computer Sciences Corporation, Falls Church VA, 30 May 1985.

56. Siegel, Sidney. Nonparametric Statistics for the Behavioral Sciences. New York: McGraw-Hill Book Company, Inc., 1956.

57. Speed, Al, 1st Information Systems Group/TPRS. Telephone interview. Pentagon, Washington DC, 24 May 1985.

58. Stein, Herman, Joint Data Systems Support Center. Telephone interview. Pentagon, Washington DC, 20 May 1985.

59. Steppel, Sam, Vice President Technology. Telephone interview. Computer Sciences Corp., Falls Church VA, 22 July 1985.

60. Sudman, Seymour and Norman H. Bradburn. Asking Questions. San Francisco: Jossey-Bass Publishers, 1983.

61. Sudman, Seymour. Reducing the Cost of Surveys. Chicago: Aldine Publishing Co., 1967.

62. The Restricted Access Processor (RAP). Product Description. Systems Division, Computer Sciences Corp., Falls Church VA, undated.

63. Turn, Reid, Ph.D. Advances in Computer System Security, Vol II. Dedham: Artech House Inc., 1984.

64. Yeskey, Donald J., Chief DOD Systems Evaluation Branch. Telephone interview. DOD Compter Security Center, Fort George G. Meade MD, 16 July 1985.

65. Yoshpe, Harry B. Production: The Industrial Sector in Peace and War. Industrial College of the Armed Forces, Washington DC, 1966.

66. Yoshpe, Harry B. and Charles F. Franke. Production for Defense. Industrial College of the Armed Forces, Washington DC, 1968.

67. Zimmerman, Don, Vice President, Telephone interview. Synergy Inc., Washington DC, 21 May 1985.

VITA

Captain Alan C. Jones was born on 12 April 1953 in Everett, Massachusetts. He graduated from Stoneham High School in Stoneham, Massachusetts in 1971 and attended Hamilton College in Clinton, New York from which he received the degree of Bachelor of Arts in Biology in June 1975. Upon graduation, he served as a Peace Corp Volunteer in the Philippines from September 1975 until November 1978. He received his commission in the USAF on 23 January 1980 upon graduating from OTS and served as the Munitions Accountable Supply Officer in the 380th Munitions Maintenance Squadron at Plattsburgh AFB, New York from from February 1980 until May 1983. His next assignment, before arriving at the Air Force Institute of Technology, was as the Munitions Accountable Supply Officer in Detachment 3 of the 425th Munitions Support Squadron, Bagotville Canadian Forces Base, Quebec, Canada from June 1983 until May 1984.

Permanent Address: RFD 3 Richard Court
Raymond, New Hampshire 03077

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

REPORT DOCUMENTATION PAGE

1a. REPORT SECURITY CLASSIFICATION UNCLASSIFIED	1b. RESTRICTIVE MARKINGS
2a. SECURITY CLASSIFICATION AUTHORITY	3. DISTRIBUTION/AVAILABILITY OF REPORT Approved for public release; distribution unlimited
2b. DECLASSIFICATION/DOWNGRADING SCHEDULE	
4. PERFORMING ORGANIZATION REPORT NUMBER(S) AFIT/GLM/LSM/85S-39	5. MONITORING ORGANIZATION REPORT NUMBER(S)
6a. NAME OF PERFORMING ORGANIZATION School of Systems and Logistics 6b. OFFICE SYMBOL (If applicable) AFIT/LSM	7a. NAME OF MONITORING ORGANIZATION
6c. ADDRESS (City, State and ZIP Code) Air Force Institute of Technology Wright-Patterson AFB, OH 45433	7b. ADDRESS (City, State and ZIP Code)
8a. NAME OF FUNDING/SPONSORING ORGANIZATION Ogden Air Logistics Center 8b. OFFICE SYMBOL (If applicable) MMWD	9. PROCUREMENT INSTRUMENT IDENTIFICATION NUMBER
8c. ADDRESS (City, State and ZIP Code) Hill AFB Ogden, UT 84056	10. SOURCE OF FUNDING NOS. PROGRAM ELEMENT NO. / PROJECT NO. / TASK NO. / WORK UNIT NO.
11. TITLE (Include Security Classification) See Box 19	
12. PERSONAL AUTHOR(S) Alan C. Jones, B.A., Capt, USAF	
13a. TYPE OF REPORT MS Thesis 13b. TIME COVERED FROM _____ TO _____	14. DATE OF REPORT (Yr., Mo., Day) 1985 September 15. PAGE COUNT 141
16. SUPPLEMENTARY NOTATION	

17. COSATI CODES		
FIELD	GROUP	SUB. GR.
17	02	
15	05	

18. SUBJECT TERMS (Continue on reverse if necessary and identify by block number)
Secure Communications, computer applications, access command and control systems, inventory control, ammunition

19. ABSTRACT (Continue on reverse if necessary and identify by block number)

Title: INTERFACING THE DEFENSE STANDARD AMMUNITION COMPUTER SYSTEM AND THE AIR FORCE COMBAT AMMUNITION SYSTEM: A SEARCH FOR AN ALTERNATE METHOD

Thesis Chairman: Warren S. Barnes, GM-13

Approved for public release: IAW AFR 190-1.
LYNN E. WOLAVER
Dean for Research and Professional Development
Air Force Institute of Technology
Wright-Patterson AFB OH 45433

20. DISTRIBUTION/AVAILABILITY OF ABSTRACT UNCLASSIFIED/UNLIMITED ☒ SAME AS RPT. ☐ DTIC USERS ☐	21. ABSTRACT SECURITY CLASSIFICATION UNCLASSIFIED
22a. NAME OF RESPONSIBLE INDIVIDUAL Warren S. Barnes, GM-13	22b. TELEPHONE NUMBER (Include Area Code) 513-255-5023 22c. OFFICE SYMBOL AFIT/LSM

DD FORM 1473, 83 APR EDITION OF 1 JAN 73 IS OBSOLETE.

UNCLASSIFIED

SECURITY CLASSIFICATION OF THIS PAGE

Conventional ammunition management is becoming more centralized. The Army, as the Single Manager for Conventional Ammunition, is developing the Defense Standard Ammunition Computer System (DSACS) to manage wholesale conventional inventories for all Military Departments. The unclassified DSACS is intended to interface with existing service ammunition systems. The Air Force is developing the Combat Ammunition System (CAS), a Secret system which will reside within the World Wide Military Command and Control System (WWMCCS) to manage Air Force wholesale and retail munitions worldwide. To be effective each system must exchange information on a real-time basis, however, a suitable interface has not been developed. This thesis used expert opinion to determine the best method of interface. A structured telephone survey was used to interview computer experts. The interview was designed to determine the necessary requirements for a suitable interface, to determine how well current technology could support the requirements, and to survey new developments in technology. Alternatives were ranked against six criteria and the Kendall Coefficient of Concordance (W) determined the significance of the analysis. Conclusions were: (1) the major interface requirements must focus on computer security issues, (2) six fundamental security requirements must be met before an interface is considered "trusted" to link CAS and DSACS, (3) no current method can provide a real-time interactive secure interface between CAS and DSACS, (4) the Secure Communications Processor (SCOMP) and the Restricted Access Processor (RAP) are two developing alternatives which best satisfied the criteria, (5) the analysis of alternatives was unable to determine which method was clearly the best. Recommendations were: (1) Air Force and Army should reevaluate their interface requirements for CAS and DSACS. (2) both services should initiate research in multilevel secure computer technology, (3) the RAP and SCOMP should be studied carefully by both services.

END

FILMED

1-86

DTIC